ACA
0112

Bound 1939

HARVARD UNIVERSITY

LIBRARY

OF THE

MUSEUM OF COMPARATIVE ZOÖLOGY

Exchange
182

SEP 28 1927

182

MEMORIAS

DE LA

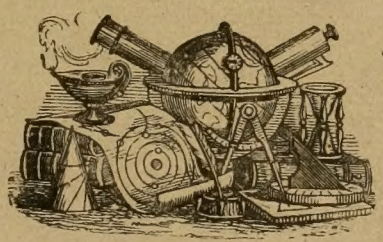
REAL ACADEMIA DE CIENCIAS

EXACTAS,

FÍSICAS Y NATURALES

DE MADRID.

TOMO VII.



MADRID:

IMPRENTA DE LA VIUDA DE AGUADO É HIJO.—PONTEJOS, 8.

1877.

LIBRARY
MUS. COMP. ZOOLOGY
HARVARD

ERRATAS CONOCIDAS, MÁS IMPORTANTES.

Página.	Línea.	Dice.	Debe decir.
17	6	a^{e}	a^{de}
110	—2	como $d \Sigma d_2$	como en el $\Sigma\ d_2$
121	13	13 (mod. 5)	— 13 (mod. 5)
162	3	número primo, cualquiera	número cualquiera
162	7	$\varphi(N) = (a^{\alpha})\,\varphi(b^{\beta})\,\varphi(c^{\gamma})\,.....$	$\varphi(N) = \varphi(a^{\alpha})\,\varphi(b^{\beta})\,\varphi(c^{\gamma})\,.....$
186	10	a^{3d-2}	a^{3d-1}
187	10	a^{0} y $a^{0} = 1$	a^{s} y $a^{0} = 1$
201	—7	$\delta(d)$	$\varphi(d)$
213	3	$g^{p-1} = 1$	$g^{p-1} \equiv 1$
222	4	raiz primitiva	raiz primitiva, impar.
222	—8	$x^{d'} = 1$	$x^{d'} \equiv 1$
271	12	$a^{2} \equiv$	$x^{2} \equiv$
305	—1	$\equiv$ (mod. 64)	$\equiv 1$ (mod. 64)
314	7	$\pm P \equiv 1$ (mod. P)	$\pm P \equiv 1$ (mod. 4)
321	—4	$D = -b$	$D = -6$
523	9	μ	n
549	—1	y este mismo	y, por tanto,
564	—3	$\sqrt{-D},\quad \sqrt{-D'}$	$\sqrt{-D} : \sqrt{-D'}$
673	—8	$N \equiv g^{s}$	$N \equiv g_{s}$

SEP 28 1927

MEMORIAS

DE LA

REAL ACADEMIA DE CIENCIAS

EXACTAS, FÍSICAS Y NATURALES

DE MADRID.

QB52
.A11

MEMORIAS

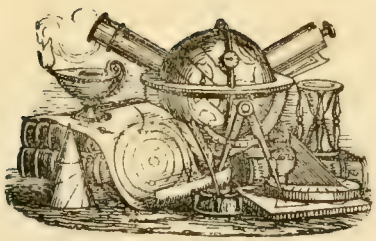
DE LA

REAL ACADEMIA DE CIENCIAS

EXACTAS, FÍSICAS Y NATURALES

DE MADRID.

TOMO VII.



MADRID:

IMPRENTA DE LA VIUDA DE AGUADO É HIJO.—PONTEJOS. 8.

1877.

Publicado por acuerdo de la Academia.

El Secretario perpétuo,

Antonio Aguilar.

TRATADO ELEMENTAL

DE LA

TEORÍA DE LOS NÚMEROS.

TEMA

PARA LA ADJUDICACION DE PREMIOS EN EL AÑO DE 1872.

«*Escribir una* Obra *sobre la* Teoría de los Números, *en la que »se presente bajo forma didáctica el estado actual de esta rama im- »portantísima de las ciencias matemáticas, y que pueda servir de »preparacion para el estudio de las* Memorias *especiales que acer- »ca de esta materia se han escrito.*»

TRATADO ELEMENTAL

DE LA

TEORÍA DE LOS NÚMEROS,

POR

DON EULOGIO JIMENEZ.

OBRA PREMIADA, EN PÚBLICO CERTÁMEN,

POR LA REAL ACADEMIA DE CIENCIAS

EXACTAS, FÍSICAS Y NATURALES.

MADRID:

IMPRENTA DE LA VIUDA DE AGUADO É HIJO.—PONTEJOS. 8.

1877.

PRÓLOGO.

La designacion por la Academia de Ciencias Exactas, Físicas y Naturales, como asunto de utilidad incuestionable y digno de premio, del tema sobre que versa este libro, nos dispensa buenamente de escribir una palabra más acerca del interes que inspira en los hombres de ciencia esta rama importantísima de las Matemáticas, que se llama, de no mucho tiempo acá, *Teoría de los Números*. Iniciado su estudio por Diofanto en la resolucion de las ecuaciones que llevan su nombre, y proseguido con éxito, muchos siglos despues, por Euler y Legendre, los problemas que hoy comprende—gracias en primer término á las investigaciones de Gauss, y á los trabajos posteriores de Lejeune-Dirichlet, Poinsot, Kummer, Eisenstein, Schwarz, Liouville, Lebesgue, Dedekind, Krönecker, y otros eminentes matemáticos—constituyen un verdadero cuerpo de doctrina, si no completo todavía, hasta cierto punto bien definido: en el cual se descubren, y explican con sorprendente claridad, relaciones no vislumbradas ántes, aunque muy íntimas y fecundas, entre asuntos al parecer inconexos de la Aritmética y el Análisis, del Algebra y la Geometría. Y por lo que á su peculiar carácter se refiere, podemos tambien afirmar, ampliando una idea de Hankel, que la *Teoría de los Números* guarda con la *Aritmética propiamente dicha* casi la misma dependencia ó semejanza que la *Geometría*, llamada *superior*, ó de *Steiner*, con la denominada *elemental*, ó de *Euclides*.

Para corroborar lo dicho, y mostrar mejor el enlace de las partes entre sí, y con el todo, hemos dividido en *tres* este libro.

En la primera parte, con el título de *Principios fundamentales*, se trata, en general, del Número y de sus *Formas;* se expone el modo como se establecen, por relacion de igualdad, las Formas numéricas, en la Aritmética vulgar ú ordinaria, ya tomando explícitamente por base el concepto cuantitativo, ya mirando al órden de los elementos de que se componen; y se indica, por último, cómo se desentrañan, en la Teoría de los Números, penetrando para ello en su organismo é íntima estructura, hasta encontrar lo que de esencial y comun poseen todas: ó la Forma final y superior que las sintetiza, y de la cual, segun el principio de la permanencia en las leyes formales, pueden como subalternas desprenderse. Este fin de la Ciencia pide, ante todo, que se determinen, respecto de ciertos tipos de comparacion, ó *módulos*, los caracteres de los números, para así clasificarlos y distribuirlos en grupos que representarán en conjunto el mismo papel que uno solo de los individuos en ellos comprendidos.

Estudiados los números aisladamente, como materiales de construccion, y sus más sencillas relaciones, procede buscar otras, fundadas en los mismos principios, pero de órden más elevado, que deslinden bajo nuevos conceptos los grupos numéricos, por las primeras constituidos. Y así como el Álgebra, supuesta la igualdad entre las formas instituidas por la Aritmética, inquiere y examina las condiciones necesarias y suficientes á que deben satisfacer los diversos elementos de aquellas formas, para que tal supuesto se realice, en la *Resolucion de las Ecuaciones;* así la Teoría de los Números, dada la congruencia de dos cantidades respecto á un módulo, investiga los caracteres de conexion, ó lazos de analogía, entre las formas posibles de aquellas cantidades y el módulo, en la *Resolucion de las Congruencias.* Y de esto precisamente trata la segunda parte de nuestro libro: en la cual hemos comprendido las proposiciones elementales, y de carácter general, acerca de las congruencias; y, como ampliacion ó complemento, la teoría más detallada de las congruencias binomias, y entre ellas, especialmente, de las de segundo grado. En esta parte además consagramos un capítulo, el último, á la *teoría de la division del círculo,* segun Gauss; no sólo porque se funda tal doctrina en una propiedad notable de las raices de la congruencia binomia, respecto de un módulo primo; sino para evidenciar la conexion admirable, como dice el mismo Gauss, entre los conceptos de la extension y del número; y probar la utilidad práctica de las investigaciones aritméticas. El estudio de la division del círculo explica y esclarece

tambien el sentido y la representacion de las cantidades *complejas*, constituidas por raices de ecuaciones binomias, y que deben considerarse como instrumentos fecundos de generalizacion, destinados á eslabonar y compendiar, conforme esperan eminentes geómetras, en muy pocos principios, muchos, hoy sin trabazon expresa, de los que comprenden las ciencias matemáticas.

Cimentada en la segunda parte, y aún esencialmente inclusa en ella, la tercera, que abraza la *Teoría de las Formas cuadráticas*, constituye principalmente por sí sola, en su propio y genuino carácter, la rama de las Matemáticas á que está consagrado este libro.

La Teoría de las *Formas cuadráticas* comprende, en efecto, la construccion ó representacion de todos los números por aquellas formas. Y las ideas apuntadas, y como en gérmen, en los comienzos del libro, y más minuciosamente desenvueltas en su segunda parte, adquieren en la tercera, hasta donde la ciencia matemática, aún en vía de progreso, permite que lo adquieran, su natural y completo desarrollo. Las formas numéricas, en un principio definidas ó consideradas como simples números aislados, ó como individualidades múltiples, sin dependencia concreta y precisa, se comparan, caracterizan y relacionan luégo, mediante tipos ó módulos conocidos, y figuran últimamente restringidas y condicionadas por *determinantes* de propiedades invariables, pero libres de cuanto en ellas existiera de vaguedad ó incertidumbre, y dispuestas, en consecuencia, para ser distribuidas, sin ambigüedad ni dudas, en clases bien marcadas, cuyo número, para cada determinante elegida, ha logrado expresar el ilustre Dirichlet, analíticamente, de un modo explícito, valiéndose para ello del poderoso auxilio del Cálculo infinitesimal.

Las dificultades que hemos tenido que vencer para desenvolver el argumento, en estas breves líneas bosquejado, y redactar una obra elemental sobre asunto tan elevado y complejo, eran bien conocidas por la Academia, como en su programa se declara. Memorias, libros, artículos....., muchos y de no escaso valer, habian visto ya la luz pública antes de comenzar nuestro trabajo; pero ninguno en castellano, ni á propósito para ser traducido á nuestro idioma, sin notables alteraciones en el fondo y en la forma, si habia de corresponder á los deseos generosos por aquella ilustre Corporacion manifestados.

Lo que pedia la Academia era una obra consagrada á exponer el estado actual de la parte de las Matemáticas, denominada *Teoría de los Números;* á facilitar la lectura de las magistrales en que se halla esta doc-

trina ampliamente tratada y discutida; y, muy principalmente, á difundir en España un órden fecundo de ideas matemáticas, hasta el presente, para la mayoría de los jóvenes que al estudio de las ciencias exactas se dedican, casi de todo punto desconocido: y á satisfacer aquella legítima peticion hemos consagrado nuestros esfuerzos, sin prescindir por completo de nuestro propio criterio al diseñar el plan de la obra. Por eso en el presente libro, verdaderamente elemental, dado su carácter, y didáctico, nos hemos atrevido á incluir teorías y principios no absolutamente necesarios para el desenvolvimiento lógico de su primordial objeto; mas de importancia reconocida, de interes general para la Matemática, y dignos, á nuestro juicio, de no ser calificados de supérfluos por nuestros benévolos lectores.

Que al proceder de este modo, apilando los materiales reunidos en largo tiempo de tenaz lectura, con ánimo de elegir lo mejor, no hemos sido de todo punto desacertados, lo demuestra el fallo favorable de la Academia: dictado seguramente, no como premio ú honra merecida, sino más bien como graciosa recompensa á nuestro buen deseo, y como estímulo para que otras personas, más competentes, prosigan, con gran provecho para la Ciencia en nuestra pátria, el trabajo por nosotros comenzado.

PARTE PRIMERA.

PRINCIPIOS FUNDAMENTALES

DE LA

TEORÍA DE LOS NÚMEROS.

CAPITULO I.

De la Aritmética propiamente dicha.—Cómo se consideran y estudian los Números en esta parte de la Matemática.

1.—*Magnitud, cantidad, número.*

La idea de número, en general, se despierta en nosotros por la contemplacion de objetos distintos. Mas estos objetos, entre otros vários modos, pueden determinarse, ya por su colocacion relativa, ya teniendo en cuenta, además de su situacion, y áun aparte de ella, ciertos caracteres comunes á todos, en los cuales se funda exclusivamente su cualidad de *homogéneos*.

Esta cualidad nos permite considerar una série, ó conjunto de cosas, como resultado de la repeticion en su posicion de cualquiera de ellas, y áun concebir una sola cosa como producto de la aglomeracion sucesiva de otra de su misma especie, cuya repeticion, hasta formar el total de la primera, determina el tamaño relativo de ambas.

Siempre que un conjunto de objetos, ó un objeto solo, puedan efectivamente mirarse como un todo constituido por la repeticion de algun otro objeto, de su especie, se dice que tal conjunto, ó tal entidad,

es una *magnitud*. El objeto cuya repetida posicion ó aglomeracion compone la magnitud se llama *unidad;* la magnitud por ésta determinada toma entonces el nombre de *cantidad;* y la determinacion de la cantidad por la unidad se llama, segun los casos, *medir* ó *contar*.

Los signos representativos de los resultados de estas dos determinaciones se denominan *números*. Estos números, por consecuencia, ó expresan, en un caso, *cuántas veces* se ejecuta, ó piensa, un acto cualquiera, y se hallan sujetos entónces á la sencilla condicion de ser una multitud de unidades (*cardinales*), ó á la doble de indicar además el lugar que tal multitud ocupa en la escala de la pluralidad (*ordinales*); ó bien representan, en otro, las veces que un objeto sensible se haya debido juntar consigo mismo para formar un total igual á otro objeto con aquel comparado. En el primero, los números son esencialmente *enteros*, su unidad es abstracta, indivisible é invariable, habiendo desaparecido de su concepto toda idea de sustancia, y se denominan vulgarmente *abstractos* ó *absolutos;* pero la unidad á que los números se refieren, en el segundo, conserva su carácter concreto, sus cualidades sustanciales, y es, en general, divisible y variable, por cuya razon se llaman *concretos*. Sólo en este sentido pueden los números, por extension, representar las cantidades.

2.—*Números enteros, fraccionarios é inconmensurables.*

Designada la unidad (concreta) en la determinacion de estos números, en el sentido de ser símbolos expresivos de relaciones cuantitativas, resultados de una medicion, pueden ocurrir tres cosas:

1.ª Que la magnitud que se trata de medir contenga á su unidad un número exacto de veces.

2.ª Que no contenga un número exacto de veces á la unidad entera, pero sí á una parte cualquiera de la misma dividida en partes iguales.

3.ª Que no contenga exactamente á la unidad entera, ni á ninguna de sus partes, por pequeñísimas que éstas se supongan.

La cantidad resultante en el primer caso, se llama *entera;* en el segundo, *fraccionaria;* en el tercero, *inconmensurable:* denominaciones que, comprensibles sólo en el terreno *concreto*, han invadido, sin embargo, el *abstracto* para aplicarse tambien á los *números*.

3.—Aritmética.—*Su objeto.*

Para patentizar el alcance de éstas y otras denominaciones del número, en su doble carácter de abstracto y concreto, la extension que sucesivamente nos veremos precisados á conceder al significado genuino de aquella palabra, y los artificios y recursos, de forma y fondo, á que necesitaremos apelar á fin de armonizar todos los conceptos del número con la propia índole de la *Aritmética*, en sus dos sentidos de *particular* (numérica) y *universal* (simbólica), recorreremos brevemente las dos partes que hoy constituyen esta *Ciencia*, á saber: las *Operaciones de cálculo*, y las *Operaciones coordinatorias*. Estas dos partes corresponden al doble carácter que envuelve la idea de número: en la primera se atiende á las cualidades de los objetos numerados, y en la segunda al órden de estos mismos. Para expresar los resultados de las primeras operaciones hacen falta diversas clases de números: para expresar los de las operaciones coordinatorias, los números enteros (los verdaderos números abstractos) solamente.

4.—Operaciones de cálculo.—*Séries fundamentales.*

Las cantidades aritméticas, propiamente dichas, son por esencia homogéneas: resultados de la repeticion de un objeto solo que, juntándose consigo mismo sucesivamente, engendra las *séries fundamentales*.

La série fundamental cuyo objeto ó unidad generatriz es el *uno* (la unidad abstracta) se llama especialmente *aritmética*, conforme con la etimología de esta palabra; y *entera* ó *natural*, segun su naturaleza y modo de constituirse.

Las *Operaciones de cálculo* se dividen en dos clases, de *agregacion* y de *disgregacion:* en la primera figuran la *adicion*, la *multiplicacion* y la *elevacion á potencias;* en la segunda, la *sustraccion,* la *division,* la *extraccion de raices* y el *cálculo logarítmico*. La *adicion, sustraccion*, *multiplicacion* y *division* se llaman tambien *fundamentales;* las otras tres *superiores*.

5.—*Adicion.*

Sumar un número a con otro b es lo mismo que tomar la unidad a veces y juntar despues con estas a unidades otras b veces la unidad. El procedimiento que se usa en esta operacion es igual al indicado anteriormente para formar la série fundamental numérica entera

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8\ldots\ldots \qquad (1)$$

por agregaciones sucesivas del *uno*.

Esta operacion produce un solo resultado ó *suma* determinada, y sus leyes fundamentales están expresadas en las igualdades siguientes:

$$a+(b+c)=(a+b)+c=a+b+c\,,$$

y

$$a+b=b+a\,:$$

la primera de las cuales se refiere á la *asociacion* y la segunda á la *conmutacion* de los *sumandos*.

6.—*Multiplicacion.*

Esta operacion se funda en el enlace de un número ordinal b con otro cardinal a, y expresa que el primero debe tomarse por sumando tantas veces como unidades contiene el segundo.

El resultado de esta operacion, el *producto* $a\,b$, puede considerarse como número formado por el *factor* b de igual manera que lo está el otro *factor* a por la unidad numérica.

Tratándose de números absolutos, goza tambien esta operacion de las mismas propiedades, *asociativa* y *conmutativa*, que la adicion, y produce, como ella, un resultado determinado; pero, enlazadas ambas, posee además la multiplicacion la propiedad que se denomina *distributiva*.

Estableciendo la igualdad necesaria

$$1 \,.\, a = a \,,$$

todas las propiedades de la multiplicacion sola, y enlazada con la adicion, se expresan como sigue:

$$a \,.\, (b \,.\, c) = (a \,.\, b \,.)\, c = a \,.\, b \,.\, c \qquad \text{(asociativa)}$$

$$a \,.\, b = b \,.\, a \qquad \text{(conmutativa)}$$

$$(b + c) \,.\, a = b \,.\, a + c \,.\, a$$
$$a \,.\, (b + c) = a \,.\, b + a \,.\, c \qquad \text{(distributiva)}$$

7.—*Sustraccion.*

Enseña á encontrar uno de dos *sumandos*, dada su *suma* y el otro *sumando;* ó bien, expresándonos simbólicamente, á deducir el valor de x de la ecuacion

$$x + b = c.$$

Segun las propiedades de la adicion anteriormente explicadas, solo un valor de x existe que satisfaga á la ecuacion

$$x + b = c \,,$$

que es el designado por la igualdad

$$x = c - b.$$

8.—*Números negativos.*

Se comprende bien pronto que cuando sea $b > c$, ningun número x existe en la série (1) entera

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7.\ldots,$$

que resuelva la cuestion de que tratamos: es decir, la sustraccion, dentro de los límites de esta série, es *imposible*. En este caso, sin embargo, la *diferencia* x, definida completamente por la igualdad

$$(c-b)+b=c,$$

puede considerarse, sin que envuelva este nuevo concepto contradiccion alguna, como un símbolo que resuelve el problema propuesto, y con el cual podremos operar como si fuese un término de la série numérica expresada.

La variabilidad de los números b y c parece, pues, que exige el establecimiento de una nueva série que comprenda los resultados de la sustraccion, siempre que sea $b>c$; mas, si admitimos la existencia de un símbolo 0 que satisfaga á la igualdad $a+0=a$, y hacemos, por consecuencia,

$$(a-a)=0,\quad (b-b)=0,\quad (c-c)=0,\ \text{etc.},$$

y convenimos en escribir, en lugar de $0-x$, el símbolo $-x$ solamente, esta série, aparentemente nueva, y la antes establecida, pueden reunirse en una sola que, comenzando por el origen comun 0, se prolongue hácia la izquierda tantos lugares como hácia la derecha, marcados unos y otros con los mismos índices 1, 2, 3, 4....., pero anteponiendo á los primeros el signo —. Esta série ampliada se expresará del modo siguiente:

$$\ldots\ldots-6,\ -5,\ -4,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6\ldots\ldots;$$

aquellos de sus términos que están á la derecha del 0 se llaman *positivos*, y los que se hallan á la izquierda del mismo origen, con el signo —, *negativos*.

9.—*Division.*

Enseña á encontrar uno de dos *factores*, dado su *producto* y el otro *factor;* ó bien, simbólicamente, á deducir el valor de x, de la ecuacion

$$x \,.\, a = b\,,$$

cuyo valor, denominado *cociente*, se expresará por la igualdad

$$x = \frac{b}{a}\,.$$

10.—*Números fraccionarios.*

Siendo a y b dos términos de la série fundamental numérica (1), se concibe fácilmente que no siempre será x tambien un término de la misma. En este caso, el *cociente* x, definido completamente por la igualdad

$$\frac{b}{a}\, a = b.$$

expresará una operacion impracticable, segun la idea que acerca de la multiplicacion expusimos en su lugar oportuno; mas, si consideramos dividida la unidad en a partes iguales, y tomamos, como nueva unidad, una de éstas, $\frac{1}{a}$, los nuevos números *fraccionarios*, $\frac{b}{a}$, quedarán tambien comprendidos en la definicion dada antes de la multiplicacion, expresando así el cociente

$$\frac{b}{a} = b\,\frac{1}{a}$$

que la unidad subalterna, $\frac{1}{a}$, debe tomarse por sumando, ó repetirse, b veces.

Si á esto agregamos que la multiplicacion indicada, $\frac{1}{a} . b$, represente la operacion de dividir la cantidad b en a partes iguales, podremos escribir sin inconveniente:

$$b . \frac{1}{a} = \frac{1}{a} . b = \frac{b}{a} ;$$

lo cual manifiesta que, en tal caso, tiene tambien lugar el principio *conmutativo*.

Estos nuevos *números fraccionarios*, ó *quebrados*, originados en la operacion de que ahora se trata, tampoco se encuentran explícitamente incluidos en la série fundamental numérica; pero pueden facilmente incluirse en ella, amplificándola entonces como sigue:

$$0, \frac{n-(n-1)}{n} \ldots\ldots \frac{n-1}{n}, 1, \frac{n+1}{n}, \frac{n+2}{n}, \frac{n+3}{n} \ldots\ldots \frac{2n-1}{n},$$

$$2, \frac{2n+1}{n} \ldots\ldots \frac{3n-1}{n}, \quad 3 \ldots\ldots$$

11.—*Elevacion á potencias.*

Como de la *adicion* se pasa á la *multiplicacion*, suponiendo iguales los sumandos, así de la *multiplicacion* se pasa á la *elevacion á potencias*, suponiendo iguales los factores.

Dos números a y n, relacionados por el algoritmo de esta nueva operacion, deben satisfacer á las condiciones siguientes: 1.ª la de producir un resultado igual á la *unidad*, cuando uno de ellos, el n, por ejemplo, sea igual á *cero;* y 2.ª la de producir un resultado igual al inmediatamente anterior, multiplicado por a, cuando el n, cualquiera que sea en el caso precedente, aumente en otra unidad.

Estas dos condiciones ó propiedades fundamentales de esta operacion se expresan simbólicamente de este modo:

$$a^0 = 1$$

$$a^{n+1} = a^n . a.$$

El número a, se llama *base;* el número n, *exponente;* el resultado de la operacion, a^n, *potencia.*

En esta operacion no se verifica el principio *conmutativo*, pues, en general, no es igual a^n que n^a; ni el *asociativo,* porque no es lo mismo $a^{(b^c)}$ que $(a^b)^c$; pero sí las leyes que se expresan en las igualdades siguientes:

$$a^{b.c} = (a^b)^c$$

$$(b\,c)^a = b^a\, c^a$$

$$a^{b+c} = a^b\, a^c$$

que corresponden al principio *distributivo.*

En la igualdad

$$a^x = c\,.$$

podemos suponer que la incógnita sea c, que lo sea a ó que lo sea n.

Si la incógnita fuese $c = x$, como implícitamente se supone hasta aquí, a entero ó fraccionario, y n entero, los resultados, x, de elevar el número a al exponente entero n se encontrarian en la série numé-

rica, amplificada (10), que encierra todos los números, enteros y fraccionarios, únicos que arroja la elevacion á una potencia entera de una base entera ó fraccionaria; puesto que toda potencia entera de un número entero ó fraccionario, es entera ó fraccionaria.

El exponente n es esencialmente entero (2), y sería absurdo suponer otra cosa en el caso de que ahora se trata.

12.—*Extraccion de raices.*

Si la incógnita fuese $a = x$, la solucion de la ecuacion

$$x^n - c$$

se expresaria por el nuevo signo

$$x = \sqrt[n]{c},$$

que se lee: *raiz n de c.*

Ahora bien, segun lo que acabamos de decir, si c es entero, su raiz x será entera; y, si no fuese esta raiz entera, tampoco podria ser fraccionaria: de donde se infiere que, mientras no sea c una potencia, entera ó fraccionaria, de exponente ó grado igual al índice n de su raiz, los números *radicales* x, esto es, las raices de los números c, ni serán enteros ni quebrados.

13.—*Números irracionales.*

La extraccion de raices exige, por consecuencia, para representar sus resultados, la creacion de nuevos símbolos que, dentro del campo de los números, llevan el nombre de *irracionales*, los cuales, no solo se distinguen de cualesquiera otros por el signo radical $\sqrt{\ }$, sino que, sin duda, para que su irracionalidad resalte todavia más, se expresan tam-

bien como potencias con exponentes fraccionarios, de modo que:

$$\sqrt[n]{c} = c^{\frac{1}{n}}.$$

Con tal artificio se enlazan estos signos entre sí, y con los demás ya definidos, mediante los algoritmos explicados; mas no bastan estas relaciones puramente formales en la estima y representacion aritmética de aquellos signos. ¿Cómo, pues, manejaremos aritméticamente los números irracionales?

Segun las definiciones dadas en el párrafo (2), y el modo de constituir la série (10), se comprende fácilmente que los números que la forman son todos *conmensurables;* y de lo dicho en este mismo párrafo se colige, que áun cuando hiciéramos crecer el número de los términos de la série (10) mencionada, y aproximarse unos á otros tanto, que la diferencia entre cada dos consecutivos llegara á ser menor que cualquiera cantidad pequeñísima dada, en lo cual no habria inconveniente, no lograríamos que alcanzasen su completa expresion en ella los números irracionales, que, por tal y tan justo motivo, se denominan tambien *inconmensurables* (2).

Pero no es difícil de concebir ahora tampoco que todo número inconmensurable puede considerarse comprendido entre dos conmensurables, muy poco, tan poco como queramos, diferentes uno de otro, y, por consecuencia, ménos todavia de aquél entre ambos comprendido, y que entónces cualquiera de ellos aproximadamente representa. Los números conmensurables así determinados respecto de los inconmensurables, son los que efectivamente caben en el campo de la Aritmética.

Mediante estos números conmensurables, como aproximaciones de los irracionales, pueden rellenarse los huecos existentes entre los términos de la série (10), hasta el punto de transformarla casi en una verdadera série ó fluencia de términos, variables por discontinuidad apenas perceptible.

14.—*Cálculo logarítmico.*

Supongamos ahora que la incógnita sea n en la igualdad que venimos examinando, y que tratamos de hallar, mediante la ecuacion

$$a^x = c\,,$$

el exponente x á que debe elevarse la base a para que el resultado de tal elevacion sea c: habremos de verificar una nueva operacion, ó *calcular el logaritmo* de un número c, de base a; y la solucion de la ecuacion propuesta se expresará como sigue:

$$x = \log_a c$$

El modo de hallar efectivamente este logaritmo se deduce de su definicion simbólica

$$a^{\log_a c} = c.$$

Basta para ello formar las potencias sucesivas de la base a,

$$a^0,\ a^1,\ a^2,\ a^3,\ a^4 \ldots\ldots,$$

y el exponente de la que sea igual al número c será el logaritmo de este número, de base a.

Conforme á los principios expuestos (11) y (12), los números que sean potencias del que haga de base, son los únicos cuyos logaritmos son racionales y enteros; mas desde el momento que miremos todos los números, sin distincion, como potencias de uno constante, los números comprendidos entre las potencias de éste deberán tener logaritmos irracionales ó inconmensurables.

Es evidente que variando la base obtendríamos tantos sistemas de logaritmos como quisiéramos; pero en todos ellos sería el logaritmo de la unidad *cero*, y la *unidad* el logaritmo de la *base*.

15.—*Gradacion de las operaciones de cálculo.*

De las ideas que dejamos apuntadas en los párrafos anteriores se infiere que todas las operaciones aritméticas se clasifican en tres categorías, entrando en cada una de ellas una operacion agregatoria, y una ó

dos disgregatorias. A la *primera* categoría corresponden la *adicion* y la *sustraccion;* en la *segunda* figuran la *multiplicacion* y la *division;* constituyen la *tercera* la *elevacion á potencias*, y la *extraccion de raices* y el *cálculo logarítmico.*

Resumiendo los principios indicados oportunamente acerca de las dos clases (4) de estas operaciones, diremos:

Sumar con el número a el número b, es agregar al a la unidad b veces; *multiplicar* a por b, es agregar al 0 el sumando a sucesivamente b veces; *elevar* a, *á la potencia* b, es agregar al 1 el factor a sucesivamente b veces. Así, por ejemplo, tenemos

$$6+4=6+(1+1+1+1)=6+1+1+1+1$$

$$6\times 4=6+6+6+6=0+(6+6+6+6)=0+6+6+6+6$$

$$6^4=6\times 6\times 6\times 6=1\times(6.6.6.6.)=1.6.6.6.6.$$

Restar de a el número b es disgregar de a el sumando b; *dividir* a por b es disgregar de a el factor b; *extraer de* a *la raiz* b es disgregar de a el exponente b, cuya base se supone posìtiva; *calcular el logaritmo de* a, *de base* b, es disgregar de a esta base elevada á una potencia, cuyo exponente se supone positivo y entero. Así, por ejemplo:

$$729-3=(726+3)-3=726+3-3=726$$

$$729:3=(243.3):3=243.3:3=243$$

$$\sqrt[3]{729} = \sqrt[3]{9^3} = 9$$

$$\log_3 729 = \log. 3^6 = 6$$

Se sobreentiende que el factor y el exponente que se disgregan no pueden ser nulos, ni la base que se eleva al exponente-logaritmo puede ser nula, ni igual á la unidad.

Las leyes á que obedecen estas operaciones, tanto respecto del órden en que se efectúan con los datos, como del enlace ó relaciones que entre las mismas pueden establecerse, se expresan con claridad en los tres cuadros siguientes:

1.°	$a+b+c=a+c+b$	$a+b-c=a-c+b$
	$a\,.\,b\,.\,c=a\,.\,c\,.\,b$	$a\,.\,b:c=a:c\,.\,b$
	$\left(a^{b}\right)^{c}=\left(a^{c}\right)^{b}$	$\left(a^{b}\right)^{\frac{1}{c}}=\left(a^{\frac{1}{c}}\right)^{b}$

$$a-b-c=a-c-b$$

$$a:b:c \quad a:c:b$$

$$\left(a^{\frac{1}{b}}\right)^{\frac{1}{c}}=\left(a^{\frac{1}{c}}\right)^{\frac{1}{b}}$$

2.°	$a+(b+c)=a+b+c$	$a-(b+c)=a-b-c$
	$a\,.\,(b\,.\,c)=a\,.\,b\,.\,c$	$a:(b\,.\,c)=a:b:c$
	$\left(a^{bc}\right)=\left(a^{b}\right)^{c}$	$\sqrt[bc]{a}=\sqrt[c]{\sqrt[b]{a}}$
	$a+(b-c)=a+b-c$	$a-(b-c)=a+(c-b)$
	$a\,.\,\frac{b}{c}=a\,.\,b:c$	$a:\frac{b}{c}=a\,.\,\frac{c}{b}$
	$a^{\frac{b}{c}}=\sqrt[c]{a^{b}}$	$\sqrt[\frac{b}{c}]{a}=a^{\frac{c}{b}}$

3.° $(a+b)c = ac + bc$ | $(a-b)c = ac - bc$

$(ab)^c = a^c\, b^c$ | $(a:b)^c = a^c : b^c$

$\frac{a+b}{c} = \frac{a}{c} + \frac{b}{c}$ | $\frac{a-b}{c} = \frac{a}{c} - \frac{b}{c}$

$(ab)^{\frac{1}{c}} = a^{\frac{1}{c}}\, b^{\frac{1}{c}}$ | $\left(\frac{a}{b}\right)^{\frac{1}{c}} = a^{\frac{1}{c}} : b^{\frac{1}{c}}$

$\log.\,(ab) = \log.\,a + \log.\,b$ | $\log.\,\frac{a}{b} = \log.\,a - \log.\,b$

$a(b+c) = ab + ac$ | $a(b-c) = ab - ac$

$a^{b+c} = a^b \,.\, a^c$ | $a^{b-c} = a^b : a^c$

Vamos á decir ahora, en lenguaje vulgar, el alcance y gradacion respectiva de las leyes antes simbólicamente expresadas, que rigen en las diversas categorías de operaciones aritméticas; mas, para evitar toda oscuridad y generalizar en la materia, conviene advertir préviamente que las letras que figuran en las fórmulas anteriores no solo pueden representar números abstractos, sino tambien cantidades; y recordar (5) que toda cantidad puede considerarse como un producto de la unidad de medida por un número. Así, por ejemplo, si a es una cantidad, será: $a = e\alpha$; donde e representa su unidad y la letra griega α su valor numérico.

Con esta aclaracion conclúyese que las leyes de la segunda categoría se deducen de las referentes á la primera, elevando un grado las operaciones inclusas en ésta; pero dentro unas y otras, naturalmente, de la misma clase, y sustituyendo el cero por la unidad; y que las fórmulas de la segunda categoría, si en ellas figurase por lo ménos una

cantidad (concreta), pueden transformarse en las fórmulas de la tercera, excepcion hecha de los logaritmos, elevando tambien un grado, dentro de la misma clase, las operaciones correspondientes á aquella, y sustituyendo además el cero por la unidad; mas advirtiendo, respecto de la operacion exceptuada, que á ella (*calcular logaritmos*), ó á la *extraccion de raices* sube, del modo que hemos dicho, la *division*, segun que sea el divisor concreto, ó abstracto.

Así, todas las leyes de la adicion y la sustraccion están expresadas, como sabemos, en las siguientes fórmulas:

$$a+(b+c)=a+b+c\,,\quad a+b=b+a\,,\quad a-b+b=a\,,\quad a+b-b=a$$

$$a+0=a\,;$$

de donde se deduce que las referentes á las operaciones de la segunda categoría, segun lo que hemos dicho, serán estas:

$$a(bc)=abc \qquad ab=ba \qquad a:b\,.\,b=a \qquad a\,.\,b:b=a$$

$$a\,.\,1=a.$$

Nótese aquí tambien, como ya indicamos (6), que la ley de la permutacion de los factores en la multiplicacion no es en general aplicable cuando juegan cantidades (concretas), y debe sustituirse diciendo que el órden en que dicha operacion se efectúe es indiferente para el resultado. Designando, pues, por letras latinas las cantidades y por griegas los números, tendremos:

$$a(\beta\gamma)=a\beta\gamma=a\gamma\beta\,,\quad a:\beta\,.\,\beta=a\beta:\beta=a\,,\quad a\,.\,1=a$$

de las cuales se desprenden las de la division (*medicion*)

$$\frac{b\alpha}{b}=\alpha\,,\quad b\,.\,\frac{a}{b}=a$$

Las fórmulas referentes al enlace de operaciones, dentro de la misma clase, de la primera y segunda categoría, son las siguientes:

$$a(\beta+\gamma)=a\beta+a\gamma\,,\quad (a+b)\gamma=a\gamma+b\gamma\,.$$

de las cuales pueden deducirse todas las restantes.

Las correspondientes á la tercera categoría serán:

$$a^{e}=(a^{d})^{e},\quad \left(\frac{1}{a^{d}}\right)^{d}=(a^{d})^{\frac{1}{d}}=a,\quad a^{1}=a$$

$$\log_{b}(b^{d})=d,\quad b^{\log_{b} a}=a,\quad a^{d+e}=a^{d}.a^{e},\quad (ab)^{e}=a^{e}b^{e}$$

16.—*Conceptos diferentes del Número.*

La necesidad de someter tambien á las leyes por que se rigen los algoritmos aritméticos, los resultados de estos mismos, incomprensibles en el terreno numérico propiamente, nos ha obligado, como se ha visto, á buscar en el concreto representacion efectiva para los signos de imposibilidad en la verificacion de las operaciones antes definidas.

Así, respecto de los números *negativos,* hemos tenido que admitir implícitamente entre los objetos ó magnitudes mismas, cuyas relaciones de cierto género expresaban los primitivos números, otras nuevas, de posicion, calidad ó influencia recíproca. Por ejemplo, dada una série de objetos

$$A\,,\quad B\,,\quad C\,,\quad D\ldots\ldots \text{ etc.,}$$

si designamos por $+1$ la dependencia, de cualquier clase que sea, entre

$$A \text{ y } B,\quad B \text{ y } C,\quad C \text{ y } D\ldots\ldots \text{ etc.,}$$

la dependencia de la misma clase entre

B y A, C y B, D y C..... etc.,

se representará por -1.

Respecto de los *quebrados* hemos tenido que admitir la division en partes iguales, no del *uno* primitivo, indivisible, sino de la unidad concreta, del *objeto-medida;* y, en cuanto á los *irracionales* ó *inconmensurables*, hemos tenido que acudir á la idea de *límite* para manejar aritméticamente los quebrados, conmensurables, que se acercan á ellos indefinidamente, pero nunca hasta confundirse ambos.

Ahora bien, ¿alcanzarán siempre estos números, negativos, fraccionarios é irracionales, representacion efectiva? No es difícil contestar negativamente á esta pregunta, si pensamos que existen muchos objetos entre los cuales no se da oposicion de conceptos, ni se concibe dependencia invertible; y no pocos séres, individuos, que no permiten, sin perder su esencia, particion alguna: ésto por lo que toca á los números negativos y fraccionarios. En cuanto á los irracionales, su mismo nombre indica que no poseen representacion total aritmética; pero, si bien es cierto que la série de operaciones numéricas, que para valuar un número inconmensurable se necesita, es interminable, tambien lo es que tales operaciones se consideran posibles cuando el sistema de cantidades homogéneas, con el cual se opera, se supone *contínuo;* es decir, que la representacion efectiva del número irracional necesita de magnitudes contínuas; y, en efecto, la *Geometría*, que opera con estas cantidades independientemente del concepto numérico, demuestra la existencia del irracional para la *Aritmética.*

Así, por ejemplo, el número irracional $\sqrt{2}$ está representado por la hipotenusa de un triángulo isósceles cuyos catetos representan la magnitud ú objeto que sirve de unidad de medida.

Infiérese de lo dicho, que, al indagar si tales ó cuales números son ó no son posibles, no nos preocupamos de que sean lógicamente imposibles; sino de ver si existe ó nó, real y efectivamente, alguna sustancia ú objeto mediante los cuales puedan alcanzar aquellos, segun su idea, adecuada manifestacion. Por no discurrir de este modo han corrido sin contradiccion, como posibles siempre, los números fraccionarios, que pueden, sin embargo, ser en muchos casos, como hemos indicado, verdaderos imposibles en el campo, no de la lógica, sino de la representa-

cion efectiva; y otros, por el contrario, posibles, han pasado por *imaginarios.*

Estos números, compuestos de la *unidad imaginaria*

$$i = \sqrt{-1},$$

que es un irracional aritméticamente, por no existir potencias de grado par con signo negativo, se han mirado por mucho tiempo exclusivamente como meros símbolos sin correspondencia ninguna con la realidad; mas, desde que las cantidades *complejas* (enlaces de real é imaginario),

$$a + b\sqrt{-1},$$

se estudiaron más profundamente y se encontró para las mismas una construccion geométrica, y una significacion de esta clase para los resultados de sus operaciones, cambió su carácter imaginario, mirándose hoy los *números complejos* como de realidad semejante á la de los positivos y negativos.

Las consideraciones que acabamos de hacer para salvar, ú ocultar al ménos, la contradiccion de lo abstracto y concreto, contínuo y discontínuo, real é imaginario, que va envuelta en el concepto de cada una de las especies de números que hemos mencionado, demuestran que el punto de vista bajo el cual miramos tales números no pertenece á una teoría pura, independiente de la sustancia ó contenido de los objetos cuyas relaciones sean por aquellos expresadas; y de aquí se deriva tambien la necesidad de fijar clara y suficientemente el significado de los números, teniendo en cuenta los dos extremos indicados.

Para evitar, pues, la oscuridad que pudiera nacer de las denominaciones y clasificaciones numéricas ya conocidas, los matemáticos llaman hoy *trascendentes, mentales* ó *puramente formales* á los números cuyo concepto está completamente determinado, pero que no es susceptible de representacion sensible; y *actuales*, á aquellos que alcanzan propia representacion en la doctrina de las magnitudes efectivas y sus relaciones.

Otros números hay qué son intermediarios entre los dichos y que se definen completamente; pero de los cuales no se sabe, en general, de antemano si estarán ó no sujetos á una construccion visible: tales números llevan el nombre de *potenciales*, mientras exista posibilidad de convertirlos en actuales; de *mentales*, si pueden ser desde luego concebidos solamente por nuestra inteligencia y no objetivamente representados; ó de *formales*, por fin, cuando no expresan sino relaciones de esta clase.

17.—*Leyes formales.—Principio de su permanencia.*

Estas relaciones formales no comprenden sólo aquellas que existen ó pueden existir entre objetos reales (como las particulares, de oposicion, en los números negativos), sino que abrazan tambien las generales, cuya posibilidad sea independiente de nuestras limitadas representaciones empíricas, y las cuales deben considerarse establecidas áun entre objetos intelectuales y entre relaciones de éstos, para despojarlas, si se quiere, de la limitacion que pudiera caber en ellas, originada por la contingencia de su realidad objetiva. El fundamento, por consecuencia, para instituir una *Aritmética general*, cuya demostracion no comprende, aunque sí algunos ejemplos, la Aritmética ordinaria, es una teoría puramente de formas, en la cual expresarán los números relaciones entre objetos mentales, entre cosas pensadas, cuyos objetos reales sensibles, ó relaciones actuales, *podrán* tambien, pero no *deberán siempre*, representar necesariamente. Esta parte formal de las Matemáticas, que pudiera llamarse *Cálculo de los símbolos*, ó quizás propiamente *Algebra* (*), arranca de un principio capital, el de la *Permanencia de las leyes formales*, fecundo para todo el organismo matemático, y que se aplica, sin definirlo expresamente, desde que se dan los primeros pasos en el estudio de esta Ciencia.

Expliquemos en breves palabras la significacion de este *Principio*.

Sea a, b, c..... una série de objetos materiales ó mentales, ó de relaciones de los mismos; y supongamos que, ligados a y b de un modo cualquiera, pero mental y formal puramente, sea c el objeto ó relacion

(*) Segun Vallés. *Estudios filosóficos sobre la ciencia del cálculo.*

nueva que resulta de tal enlace: es claro que este resultado *c* podrá reemplazar á los dos términos *a*, *b*, en cuanto se consideren unidos, y mirarse como igual á ellos juntos, esto es, á su union, en todas las conclusiones ulteriores. Establecidos tales enlaces, sujetos á ciertas reglas, entre los resultados de enlaces ó uniones diferentes, surgirán nuevas relaciones, que se deducirán de las primitivas lógicamente, y con entera independencia de la naturaleza de las cosas enlazadas. Mas, como las reglas á que tienen que sujetarse estos encadenamientos, y que definen las operaciones que deberán efectuarse con los objetos mentales que constituyen sus términos, son arbitrarias, deberemos poner cuidado en que no vaya envuelta en ellas alguna contradiccion lógica: contingencia que podremos evitar si, al dictar dichas reglas, las establecemos tan independientes entre sí que ninguna de ellas esté contenida en otra bajo ningun concepto, y nos limitamos en su establecimiento á lo que sea suficiente.

De este modo, es óbvio que formaremos un sistema de operaciones mentales, donde éstas y los objetos á las mismas sometidos se hallarán definidos *suficientemente* nada más, y el cual, respecto de la interpretacion de sus resultados y sus aplicaciones, será absolutamente estéril. Para no llegar, pues, á parar en un sistema tan vano como abstruso, habremos de someter las operaciones con objetos mentales á reglas formales á cuyo dominio y régimen estén tambien sujetas las operaciones con objetos ó magnitudes efectivas, cuyas relaciones expresan los números ordinarios.

La *Aritmética*, en sus dos sentidos, de *particular* (de guarismos ó signos especiales) y *universal* (literal, de signos más generales, de letras), nos presenta un sistema de reglas que gozan realmente del carácter de independencia antes exigido, y nos señalan el camino para definir una operacion formal de manera, que sus resultados, dentro de la Aritmética *universal*, se conviertan en los de la *particular*, siempre que los objetos mentales, que juegan en la primera, se sustituyan por objetos actuales cuyas mútuas relaciones representen las cifras ó números vulgares. El principio comprendido en las anteriores líneas es el de la *Permanencia de las leyes formales*, que puede enunciarse de este modo:

Siempre que dos formas expresadas por signos generales de la Aritmética universal sean iguales entre sí, permanecerán tambien iguales entre sí cuando se sustituyan aquellos signos por simples cantidades; y las

operaciones, por consecuencia, en aquellas indicadas, abrazarán cualquiera otro contenido.

18.—*Aplicacion de las leyes formales.*

No es nuestro ánimo, ni sería oportuno tampoco, entretenernos aquí en desenvolver esta doctrina, y en examinar su generalidad y limitaciones, en cuanto se refiere á las diferentes propiedades de las operaciones aritméticas y áun de otras superiores; pero no dejaremos este asunto sin presentar algun ejemplo de la misma, que evidencie en parte su trascendencia, conforme á las ideas anteriormente indicadas.

Sean a, b, c tres objetos combinados, segun los algoritmos aritméticos, de tal modo, que del enlace, mediante operaciones *disgregatorias* (4), de a y b, resulte c. Este enlace de a y b, que se expresa

$$\delta(a, b) = c,$$

se caracteriza estableciendo que siempre que su resultado c se combine, mediante operaciones *agregatorias,* con uno de sus términos, b, debe resultar el otro, a, *necesariamente.* Designando por $\alpha(c, b)$ la union por agregacion de c y b, tendremos, segun lo dicho,

$$\alpha(c, b) = a,$$

ó bien

$$\alpha\{\delta(a, b), b\} = a. \qquad (1)$$

Suponemos aquí que, dados a y b, tanto las operaciones $\alpha(a, b)$, como las $\delta(a, b)$, son posibles, y tienen una sola significacion: es decir, que todos los resultados en cada una de estas dos clases opuestas de relaciones, son iguales entre sí y pueden, por lo tanto, mutuamente sustituirse.

De esta hipótesis se deducen las consecuencias siguientes:

Dada la igualdad

$$\delta(a,\ b) = \delta(a',\ b),$$

tambien necesariamente debe existir esta otra: $a = a'$; pues, si así no sucediera, tendríamos que la igualdad

$$\alpha\left\{\delta(a, b), b\right\} = \alpha\left\{\delta(a', b), b\right\}$$

sería imposible, por ser su primer miembro igual á a, y el segundo á a' (1).

Si en la operacion $\delta(a, b)$ varía el término a, permaneciendo b constante, variará necesariamente el resultado; de donde se infiere que la ecuacion

$$\delta(x,\ b) = a$$

tiene una solucion única, que se halla uniendo, mediante operaciones agregatorias, sus dos miembros con b, como sigue:

$$\alpha\left\{\delta(x,\ b), b\right\} = \alpha(a,\ b);$$

de donde (1) se deduce

$$x = \alpha(a,\ b),$$

y de aquí, la identidad

$$\delta\left\{\alpha(a,\ b), b\right\} = a. \qquad (2)$$

Cuando en las dos formas

$$\delta(a,\ b) \quad \text{y} \quad \alpha(a,\ b)$$

varíe el primer término, siendo constante el segundo, el resultado de las operaciones variará tambien; de modo que, de las dos ecuaciones

$$\delta(a, b) = \delta(a', b), \qquad \alpha(a, b) = \alpha(a', b).$$

se concluye siempre que es $a = a'$.

Si, en lugar de las hipótesis antes sentadas, admitiésemos ahora que la operacion $\alpha(a, b)$ tiene ciertamente una significacion única, y que su resultado varía siempre que lo verifique su primer término, las mismas propiedades se deducirian de tal suposicion para la operacion correspondiente $\delta(a, b)$. En efecto, si la operacion $\delta(a, b)$ produjese resultados diferentes, c, c', por ejemplo, sería

$$\alpha \{ \delta(a, b), b \} = \alpha(c, b) = \alpha(c', b) = a;$$

pero, segun lo admitido antes, la igualdad

$$\alpha(c, b) = \alpha(c' b)$$

sólo puede verificarse en el caso de ser $c' = c$: luego la operacion $\delta(a, b)$ es determinada en cuanto á su resultado, el cual variará cuando a varie.

Apliquemos estos principios á los números reales y á las operaciones ya explicadas en su lugar correspondiente, que con los mismos pueden efectuarse.

1.° Sea, pues,

$$\alpha(a, b) = a + b,$$

operacion que posee las dos propiedades de que venimos haciendo mérito: la operacion inversa será

$$\delta(a, b) = a - b,$$

puesto que

$$\alpha \{ \delta(a, b), b \} = \alpha(a - b, b) = a - b + b = a;$$

de donde se infiere que $\delta(a, b)$ es tambien determinada, y varía cuando a varie.

2.° Sea ahora

$$\alpha(a, b) = a\,b;$$

la inversa será

$$\delta(a, b) = \frac{a}{b},$$

segun la demostracion que acabamos de dar para la suma.

Puesto que el producto $a\,b$ arroja un resultado único, y varía solamente cuando a ó b varien, la operacion inversa, esto es, el cociente $\frac{a}{b}$ gozará tambien de las mismas propiedades. Pero si fuese $b = 0$, como el producto de a, y de todo otro número finito, por cero, es cero, la operacion $\frac{a}{b}$ sería indeterminada.

3.° Sea, por fin,

$$\alpha(a, b) = a^{b},$$

y la inversa

$$\delta(a, b) = c:$$

entonces será (1)

$$\alpha(c, b) = c^{b} = e^{b \log. c} = a;$$

de donde se deduce

$$c = \delta(a, b) = e^{\frac{\log. a}{b}}.$$

Tambien aquí las operaciones, directa é inversa, varian en sus resultados

cuando sus términos lo verifican; pero, cuando sea $b = o$, la operacion agregatoria a^b producirá un resultado único, cualquiera que sea el valor positivo de a; mientras que la inversa $e^{\frac{\log. a}{b}}$ será respectivamente igual á *infinito*, ó á *cero*, si a es entero, ó fraccionario, y tomará un valor *indeterminado*, en el supuesto de ser a igual á la unidad.

Deteniéndonos á pensar un poco en estos ejemplos, se nota que á cada operacion agregatoria corresponden por lo ménos dos inversas. Así, en efecto, á la suma

$$a + b = s$$

corresponden las dos restas

$$s - a \quad \text{y} \quad s - b\,;$$

al producto

$$a\,b = p\,,$$

los dos cocientes

$$\frac{p}{a} \quad \text{y} \quad \frac{p}{b}\,;$$

y á la potencia

$$a^b = P\,,$$

la raiz y el logaritmo

$$\sqrt[b]{P} \quad \text{y} \quad b = \frac{\log. P}{\log. a}\,.$$

Considerando la cuestion en general, podemos establecer que estas operaciones inversas, disgregatorias, resuelven respectivamente los dos problemas expresados en las dos ecuaciones

$$\alpha(x, b) = a, \quad \text{y} \quad \alpha(b, x) = a.$$

Refiriéndonos al caso 3.°, por ejemplo, estas dos ecuaciones tomarán la forma concreta

$$x^b = a \qquad \text{y} \qquad b^x = a;$$

la solucion de la primera será, como sabemos,

$$x = e^{\frac{\log. a}{b}};$$

la de la segunda,

$$x = \frac{\log. a}{\log. b};$$

y es evidente que estas dos soluciones coincidirian, si en las operaciones correspondientes se verificase el principio conmutativo (6) y (11), esto es, si fuese cierta la igualdad

$$\alpha(a, b) = \alpha(b, a).$$

Del mismo modo, que hemos procedido para deducir formalmente las propiedades de las operaciones de cálculo sujetas al principio *asociativo* y no al *conmutativo*, procederíamos en el exámen de las operaciones sometidas á este último; pero estas investigaciones nos llevarian muy léjos de nuestro principal propósito: por cuya razon las abandonamos para emprender otras que nos interesan más inmediatamente.

19.—Operaciones coordinatorias.—*Definiciones generales.—Notacion.*

En la *Teoría de las coordinaciones*, cuyos elementales principios vamos á exponer ahora, se atiende meramente al número y colocacion de ciertos objetos, reales ó mentales, que se miran como unidades siempre indefinidas, como puros individuos, que no se trata de aglomerar y fundir aquí, como se reunen efectivamente los elementos numéricos mediante las *Operaciones de cálculo*, sino, en general, de *ordenarlos*.

Llámase *coordinacion* un conjunto de objetos marcados por números ó letras, puestos unos al lado de otros.

El número de objetos, *elementos*, de que consta una coordinacion, determina su *clase*. Estas *clases* se llamarán *unarias*, *binarias*, *ternarias*, *cuaternarias*, etc., segun que las coordinaciones contengan *uno*, *dos*, *tres*, *cuatro*, etc., elementos.

Las coordinaciones, en cada clase, pueden diferenciarse, ó por el *órden* de sus elementos, ó por la *naturaleza* de éstos. Cuando en una misma clase no existan dos coordinaciones formadas por los mismos elementos, tomarán estas el nombre de *combinaciones* ó *productos diferentes;* y de *variaciones*, si tal limitacion desaparece.

Tanto las *variaciones* como las *combinaciones*, se dirán sin *repeticion* ó con ella, segun que no contengan, ó contengan, elementos repetidos.

Las coordinaciones resultantes de permutar todos los elementos de una coordinacion cualquiera, esto es, haciendo que cada uno de ellos ocupe sucesivamente todos los lugares posibles, se llaman *permutaciones*.

Las *permutaciones* sin repeticion, por consecuencia, *son variaciones* en las cuales el grado de la clase es igual al número total de los elementos coordinados. Las permutaciones con repeticion son las que se derivan de una coordinacion donde existen elementos repetidos.

Finalmente, en las coordinaciones con repeticion (*variaciones* y *combinaciones*) es preciso tener en cuenta si cada elemento puede repetirse tantas veces como unidades contenga el número que expresa el grado de la clase, ó si, por el contrario, deberá repetirse solamente un número de veces con antelacion señalado. En el primer caso se dice que la re-

peticion es *ilimitada*, y en el segundo, *limitada:* á la *repeticion* ilimitada nos referiremos siempre que usemos esta palabra.

El número de *variaciones*, sin repeticion, de la clase n, que pueden formarse con a elementos, se designa por a'^{n}; y por a''^{n}, si fueren con repeticion.

El número de *permutaciones* de una coordinacion formada por n elementos, todos diferentes, se expresará por $n!$; y, si en la coordinacion permutanda existieren: a elementos iguales entre sí, de una especie; b elementos iguales entre sí, de otra especie; c elementos iguales entre sí, de una tercera especie..... etc., por $(a, b, c.....)!$. El número de combinaciones, sin repeticion, de la clase n, con a elementos, se designará por $a^{.n}$; y, si fuesen con repeticion, por $a^{..n}$.

20.—*Número de variaciones sin repeticion.*

El número de variaciones, sin repeticion, de la clase n, con a elementos, es igual al producto de n términos consecutivos, de mayor á menor, de la série numérica, comenzando desde el número a.

En signos:

$$a'^{n} = a(a-1)..... \quad (a-n+1).$$

En efecto, las variaciones con a elementos de una clase cualquiera se obtienen juntando cada uno de dichos elementos sucesivamente, con las variaciones de la clase inferior, inmediata, que pueden efectuarse con los $a-1$ elementos restantes. Luego tendremos:

$$a'^{n} = a(a-1)'^{a-1}.$$

Y, aplicando el mismo razonamiento al segundo factor del segundo miembro de esta igualdad, resultará esta otra:

$$a'^{n} = a(a-1)(a-2)'^{n-2};$$

y, despues de repetido este procedimiento m veces, la siguiente

$$a'^{n} = a(a-1)\ldots\ldots (a-m+1)(a-m)'^{n-m}.$$

Haciendo ahora

$$m = n-1,$$

será por fin:

$$a'^{n} = a(a-1)\ldots\ldots (a-n+1). \qquad (1)$$

21.—*Número de permutaciones sin repeticion.*

El número de permutaciones, sin repeticion, con n elementos, es igual al producto de los n primeros términos de la série numérica.

En signos:

$$n! = 1 \,.\, 2 \,.\, 3\ldots\ldots n.$$

En efecto, las permutaciones sin repeticion, dijimos, son variaciones en las cuales el grado de la clase es igual al número total de los elementos coordinandos; luego

$$n! = n'^{n} = n(n-1)\ldots\ldots (n-n+1);$$

esto es,

$$n! = 1 \,.\, 2 \,.\, 3\ldots\ldots n. \qquad (2)$$

22.—*Número de combinaciones sin repeticion.*

El número de combinaciones, sin repeticion, de la clase n, con a elementos, es igual á un quebrado cuyo numerador expresa el número de variaciones de la misma clase y con los mismos elementos, y el denominador su número de permutaciones.

En signos:

$$a'^{n} = \frac{a'^{n}}{n!}$$

En efecto, las combinaciones, sin repeticion, de una clase cualquiera, se obtienen juntando con cada una de las combinaciones de la clase inmediata, inferior, sucesivamente, todos los elementos que no entren en ellas. Segun ésto, de las combinaciones de una clase, se obtienen las variaciones colocando sucesivamente cada uno de los elementos que existan en aquellas en todos los lugares posibles: de donde se deduce que cada combinacion produce tantas variaciones, como permutaciones pueden efectuarse con los elementos de que consta; ó bien, que el número de variaciones de una clase es tantas veces mayor que el de combinaciones de la misma clase, como permutaciones pueden formarse con un número de elementos igual al grado de la clase mencionada.

Reemplazando los símbolos del segundo miembro de la igualdad última, por las expresiones algebráicas en ellos compendiadas, resultará, por consecuencia:

$$a'^{n} = \frac{a(a-1)\ldots.(a-n+1)}{1 \cdot 2 \cdot 3 \ldots\ldots n} \qquad (3)$$

Multiplicando los dos términos del segundo miembro de esta igualdad por

$$1 \cdot 2 \cdot 3 \ldots\ldots (a-n) = (a-n)!$$

se convertirá en la que sigue:

$$a^{\cdot n} = \frac{a!}{n!\,(a-n)!}. \qquad (4)$$

Pero, como de aplicar la fórmula (3) se deduce esta otra

$$a^{\cdot a-n} = \frac{a(a-1)\ldots\ldots(n+1)}{1 \cdot 2 \ldots\ldots (a-n)},$$

la cual á su vez, multiplicando los dos términos de su segundo miembro por $n!$, se transforma en la siguiente:

$$a^{\cdot a-n} = \frac{a!}{(a-n)!\,n!},$$

resulta, por fin, la más importante de todas:

$$a^{\cdot a-a} = a^{\cdot n}. \qquad (5)$$

Esta fórmula simbólica en lenguaje vulgar, dice: que *el número de combinaciones de la clase* n, *con* a *elementos, es igual al número de las que pueden efectuarse con los mismos elementos, pero de la clase* $a-n$.

23.—*Número de combinaciones con repeticion.*

El número de combinaciones, con repeticion, de la clase n, que pueden formarse con a elementos, es igual á un quebrado, cuyo numerador es el producto de n términos consecutivos, de menor á mayor, de la série numérica comenzando por el número a, y cuyo denominador es el producto de los n primeros términos de la misma série.

En signos:

$$a^{..n} = \frac{a\,(a+1)\,.....\,a+n-1}{1\,.\,2\,.....\,n}$$

En efecto, para obtener las combinaciones con repeticion de la clase n, con a elementos, se habrán de juntar sucesivamente cada uno de los a elementos con cada una de sus combinaciones de la clase $(n-1)$, y además en cada combinacion de estas mismas cada uno de los $(n-1)$ elementos que entran en ellas.

El resultado de esta operacion, designando por $a^{..n-1}$ el número de combinaciones con a elementos de la clase $(n-1)$, segun sabemos, será:

$$a^{..n} = a\,a^{..n-1} + (n-1)\,a^{..n-1} = (a+n-1)\,a^{..n-1}.$$

Mas de este modo, cada combinacion resulta n veces repetida; y, por consecuencia, el número de las combinaciones realmente distintas será

$$a^{..n} = a^{..n-1}\,\frac{a+n-1}{n}$$

Ahora bien, es claro que

$$a^{..1} = a = \frac{a}{1};$$

de donde se deducen:

$$a^{..2} = a^{..1}\ \frac{a+1}{2} = \frac{a(a+1)}{1\ .\ 2}$$

$$a^{..3} = a^{..2}\ \frac{a+2}{3} = \frac{a(a+1)(a+2)}{1\ .\ 2\ .\ 3}$$

. . . . . .

$$a^{..n} = a^{..n-1}\ \frac{a+n-1}{n} = \frac{a(a+1)\ldots..\ (a+n-1)}{1\ .\ 2\ldots..\ n}\ . \quad (6)$$

24.—*Número de variaciones con repeticion.*

El número de variaciones, con repeticion, de la clase n, *que pueden efectuarse con* n *elementos, es igual á una potencia cuya base es el número* a *de elementos, y cuyo exponente es el número* n, *que indica el grado de la clase.*

En signos:

$$a''^{n} = a^{n}.$$

En efecto, las variaciones, con repeticion, de la clase n, con a elementos, se obtienen juntando cada uno de éstos, con cada una de las variaciones de la misma especie, de la clase $(n-1)$, que pueden hacerse con dichos a elementos. Designando, pues, como sabemos, por a''^{n-1} el número de variaciones con repeticion de la clase $(n-1)$, con a elementos, será:

$$a''^{n} = a\ .\ a''^{n-1}.$$

Aplicando esta misma ley al segundo factor del segundo miembro, tendremos:

$$a''^{n-1} = a \,.\, a''^{n-2}$$

y, sustituyendo en la primera fórmula, será:

$$a''^{n} = a \,.\, a \,.\, a''^{n-2} = a^{2} \,.\, a''^{n-2} :$$

la cual, despues de aplicar m veces el mismo procedimiento, se convierte en esta otra:

$$a''^{n} = a^{m} \,.\, a''^{n-m} .$$

Haciendo aquí

$$m = n - 1 ,$$

y, recordando que

$$a''^{1} = a ,$$

se llega, por fin, á la fórmula

$$a''^{n} = a^{n-1} \,.\, a''^{n-n+1} = a^{n-1} \,.\, a''^{1} ;$$

ó bien

$$a''^{n} = a^{n} \qquad (7)$$

25.—*Número de permutaciones con repeticion.*

El número de permutaciones, con repeticion, de n elementos, es igual á un quebrado cuyo numerador expresa el número de permutaciones de estos n elementos como si fuesen todos diferentes, y cuyo denominador es un producto de tantos factores como especies distintas de elementos existan en los n mencionados, expresando cada uno de estos factores el número de permutaciones que podrian efectuarse con los elementos iguales entre

sí, que constituyen cada una de las referidas especies, considerados como si fuesen diferentes.

En signos:

$$a, b, c.....)! = \frac{(a+b+c.....)!}{a!\,b!\,c!.....} = \frac{n!}{a!\,b!\,c!.....};$$

en cuya fórmula se supone que de los n elementos son: a iguales entre sí; b iguales entre sí, pero diferentes de los anteriores; y c iguales entre sí tambien, pero de una tercera especie, etc.

En efecto, admitamos por un momento que los n elementos son todos diferentes; señalemos a elementos cualesquiera, y distribuyamos las $n!$ permutaciones que producen los n dados en grupos, de manera que en todas las coordinaciones de cada uno de estos grupos ocupen los mismos lugares los otros elementos no señalados. Es claro que, procediendo así, en cada grupo habrá tantas permutaciones como se puedan formar con los a elementos marcados, esto es, $a!$ permutaciones, las cuales se reducirán á una sola en el momento que consideremos iguales los a elementos prefijados. Por consecuencia, el número $n!$ de permutaciones, en la hipótesis de ser los n elementos diferentes, es $a!$ veces mayor que el número de permutaciones, en el caso de ser iguales a elementos de los n dados; luego este número de permutaciones con n elementos, de los cuales sean a iguales, tendrá por expresion el cociente

$$\frac{n!}{a!}.$$

Si admitiésemos ahora que, además de los a elementos iguales de cierta especie, existieran en los n dados, b elementos iguales entre sí de otra especie, c elementos iguales entre sí de una tercera, etc., llegaríamos fácilmente, mediante el mismo razonamiento empleado para deducir el cociente anterior, á la fórmula general

$$(a, b, c.....)! = \frac{(a+b+c.....)!}{a!\,b!\,c!.....} = \frac{n!}{a!\,b!\,c!.....} \qquad (8)$$

26.—*Relaciones entre números coordinatorios.*

Entre algunos de los diferentes números coordinatorios, cuyas definiciones hemos dado, existe la dependencia expresada por las igualdades siguientes:

$$(a, b)! = (a+b)^{\cdot a} = (a+b)^{\cdot b} = (b+1)^{\cdot\cdot a} = (a+1)^{\cdot\cdot b} \qquad (9)$$

En efecto, aplicando directamente la fórmula (8) tenemos:

$$(a, b)! = \frac{(a+b)!}{a!\,b!} = \frac{1 \,.\, 2 \,.\,.\,.\,.\, (a+b)}{1 \,.\, 2 \,.\,.\,.\,.\, a \,.\, 1 \,.\, 2 \,.\,.\,.\,.\, b}.$$

Suprimiendo de los dos términos de este quebrado sus a primeros factores comunes, tendremos (23):

$$(a, b)! = \frac{(a+1)(a+2)\,.\,.\,.\,.\,(a+b)}{1 \,.\, 2 \,.\,.\,.\,.\, b} = (a+1)^{\cdot\cdot b};$$

ó bien, invirtiendo el orden de los factores del numerador (22),

$$(a, b)! = \frac{(a+b)(a+b-1)\,.\,.\,.\,.\,(a+1)}{1 \,.\, 2 \,.\,.\,.\,.\, b} = (a+b)^{\cdot b}.$$

Suprimiendo, por el contrario, en vez de los a factores antedichos, los factores $1 \,.\, 2 \,.\,.\,.\,.\, b$ en el mismo quebrado, llegaremos fácilmente á las dos fórmulas que siguen:

$$(a, b)! = \frac{(b+1)(b+2)\,.\,.\,.\,.\,(b+a)}{1 \,.\, 2 \,.\,.\,.\,.\, a} = (b+1)^{\cdot\cdot a}$$

$$(a,\ b)\,! = \frac{(a+b)\,(a+b-1)\ldots\ldots\ (b+1)}{1\,.\,2\ldots\ldots\ a} = (a+b)^{a}$$

que demuestran la presupuesta (9).

27.—*Número de todas las combinaciones posibles.*

Determinaremos, por fin, el número de todas las *combinaciones* posibles de todas clases, con repeticion ó sin ella, que pueden formarse con n elementos dados, diferentes.

Sean estos elementos

$$a^{\alpha},\ b^{\beta},\ c^{\gamma}\ldots\ldots\ l^{\lambda},\ m^{\mu},$$

donde los exponentes

$$\alpha,\ \beta,\ \gamma\ldots\ldots\ \lambda,\ \mu,$$

indican las veces que en cada combinacion pueden estar á lo más repetidos los elementos á que afectan. Es evidente que el elemento a, solo, produce las α combinaciones

$$a,\ aa,\ aaa\ldots\ldots\ \overbrace{aaaaa}^{\alpha}\ldots\ldots$$

y que el elemento b, solo, produce β; el c, solo, γ, etc.; todas de la misma especie que las anteriores de a.

Los dos elementos a y b producen, por consecuencia, $\alpha+\beta$ combinaciones de un solo elemento respectivamente; mas, si combinamos tambien las α combinaciones del elemento a solo, con cada una de las β combinaciones del elemento b solo, obtendremos $\alpha\beta$ nuevas combinaciones que contendrán los dos elementos a y b. De modo que estos dos elementos producen

$$\alpha+\beta+\alpha\beta = \alpha+(1+\alpha)\,\beta$$

combinaciones.

El elemento c, solo, como dijimos, produce γ combinaciones, á saber:

$$c,\ cc,\ ccc.....\ \overset{\smile}{ccccc}.....;$$

mas, combinando con cada una de éstas, todas las formadas antes por los a y b, resultarán

$$\gamma\{\alpha+(1+\alpha)\beta\}$$

combinaciones, en todas las cuales figurará el nuevo elemento c.

Reuniendo ahora el número de combinaciones que produjeron los dos elementos a y b, con el escrito últimamente, y con el número γ de las combinaciones que forma el elemento c, solo, obtendremos el total

$$\alpha+(1+\alpha)\beta+\gamma\{\alpha+(1+\alpha\beta\}+\gamma;$$

ó bien, sumando y restando la unidad,

$$(1+\alpha)(1+\beta)(1+\gamma)-1$$

Tomando sucesivamente otros elementos, y razonando siempre del mismo modo hasta concluir con los n diferentes, propuestos, se obtiene la expresion

$$(1+\alpha)(1+\beta)(1+\gamma).....(1+\lambda)(1+\mu)-1 \qquad (10)$$

que representa el número que buscamos.

Si los exponentes

$$\alpha,\ \beta,\ \gamma.....\ \lambda,\ \mu,$$

fuesen todos iguales á la unidad, la diferencia anterior, se convertiria en esta otra:

$$(1+1)(1+1)(1+1).....(1+1)(1+1)-1=2^n-1 \qquad (11)$$

28.—Potencia de un binomio.—*Preliminares.*

Aunque de los principios de la teoría coordinatoria, anteriormente demostrados, se deducen importantes consecuencias, principalmente aplicables al desarrollo en série de las potencias de una forma binomia; sin embargo, apartándonos del uso más comun, vamos á estudiar este desarrollo con independencia de aquella teoría, ó algo más directamente que en los libros elementales de Algebra suele verificarse. Para ello determinaremos *empíricamente* el coeficiente de la série binomia, y, sin más consideraciones extrañas al asunto, procuraremos demostrar su generalidad y exactitud.

Si, mediante las reglas conocidas de la multiplicacion, formamos las potencias sucesivas del binomio $(1+x)$, resultará el cuadro siguiente:

$$(1+x)^2 = 1+2x+x^2$$

$$(1+x)^3 = 1+3x+3x^2+x^3$$

$$(1+x)^4 = 1+4x+6x^2+4x^3+x^4$$

$$(1+x)^5 = 1+5x+10x^2+10x^3+5x^4+x^5$$

$$(1+x)^6 = 1+6x+15x^2+20x^3+15x^4+6x^5+x^6.$$

. . . . . .

Fijándonos en los coeficientes

$$1.\quad 6,\quad 15.\quad 20.\quad 15.\quad 6.\quad 1.$$

que figuran en el desarrollo de la *sexta* potencia, y dividiendo cada uno de ellos, comenzando desde el segundo, por el inmediatamente anterior, en los cocientes resultantes, simplificados,

$$\frac{6}{1}, \frac{5}{2}, \frac{4}{3}, \frac{3}{4}, \frac{2}{5}, \frac{1}{6},$$

se manifiesta una ley á que obedecen los coeficientes de todos los demás desarrollos expuestos, y con arreglo á la cual puede escribirse el de la sexta potencia elegida, de este modo significativo:

$$(1+x)^6 = 1 + \frac{6}{1}x + \frac{6.5.}{1.2}x^2 + \frac{6.5.4}{1.2.3}x^3 + \frac{6.5.4.3}{1.2.3.4}x^4 +$$

$$\frac{6.5.4.3.2}{1.2.3.4.5}x^5 + \frac{6.5.4.3.2.1}{1.2.3.4.5.6}x^6.$$

La cuestion, pues, se reduce en este momento á probar si esta ley puede ó no generalizarse para toda potencia. Para llegar á la demostracion procederemos por partes.

1.ª En primer lugar observamos que la forma general de los coeficientes fraccionarios del último desarrollo, es evidentemente

$$\frac{a(a-1)\ldots\ldots(a-n+1)}{1.2\ldots\ldots n},$$

que ya (22) designamos por el número $a^{.n}$.

Este número, por las razones allí expuestas, se llama *combinatorio;* a, su *base;* y n, su *exponente.* Prescindiendo de esta significacion, y atendiendo sólo á que representa la ley de los coeficientes del indicado desarrollo, el quebrado

$$a^{.n-1} = a^{.n} \cdot \frac{n}{a-n+1}$$

(donde n se supone entero y positivo) que se deduce facilmente del anterior, nos dará para los valores de n menores que 3, á saber,

$$n=2, \quad n=1, \quad \text{y} \quad n=0.$$

las relaciones siguientes:

$$a^{\cdot 1} = a$$

$$a^{\cdot 0} = 1$$

$$a^{\cdot -1} = 0;$$

la última de las cuales no cambiará para cualquiera otro valor de n inferior á cero, y puede, por consecuencia, escribirse de este modo:

$$a^{\cdot -n} = 0.$$

2.ª Sobre el número combinatorio $a^{\cdot n}$ emitiremos ahora algunas reflexiones, indispensables para la buena inteligencia de lo que ha de seguir.

El exponente n del número a, que siempre es entero, puede ser *negativo, nulo* ó *positivo*. En el primer caso, es,

$$a^{\cdot -n} = 0;$$

en el segundo,

$$a^{\cdot n} = a^{\cdot 0} = 1,$$

segun acabamos de demostrar; réstanos considerar el tercero, esto es, aquel en que n sea positivo.

Si n es positivo, puede ser

$$n = 1, \quad \text{ó} \quad n > 1:$$

en el primer supuesto será

$$a^{\cdot n} = a^{\cdot 1} = a,$$

y nulo, por consecuencia, sólo cuando sea $a = 0$, único entero menor que 1; en el segundo supuesto, $n > 1$, el número $a^{\cdot n}$ será un que-

brado, y nulo, por tanto, sólo en el caso de que su numerador lo sea; pero este numerador, que es el producto

$$a\,(a-1)\ldots\ldots\,(a-n+1)\,,$$

será cero cuando lo sea uno de sus factores, esto es, cuando sea $a=0$, ó bien

$$a=1\,,\quad a=2\ldots\ldots,\quad a=n-1.$$

Luego el número combinatorio $a^{\cdot n}$ será 0 solamente:

1.° *Cuando su exponente n sea negativo;*

2.° *Cuando su base a sea un número entero, no negativo, y su exponente n mayor que dicha base.*

3.° Y, por último, demostraremos que

La igualdad simbólica

$$(a+1)^{\cdot n}=a^{\cdot n}+a^{\cdot n-1} \qquad (12)$$

es cierta.

En efecto, escribiendo con los signos ordinarios algebráicos los dos términos del segundo miembro, tendremos:

$$a^{\cdot n}+a^{\cdot n-1}=\frac{a\,(a-1)\ldots\ldots\,(a-n+1)}{1\,.\,2\ldots\ldots\,n}+\frac{a\,(a-1)\ldots\ldots\,(a-n+2)}{1\,.\,2\ldots\ldots\,(n-1)}$$

$$=\frac{a\,(a-1)\ldots\ldots\,(a-n+2)\,\{a-n+1+n\}}{1\,.\,2\ldots\ldots\,n}$$

$$=\frac{(a+1)\,a\,(a-1)\ldots\ldots\,(a-n+2)}{1\,.\,2\ldots\ldots\,n}=(a+1)^{\cdot n}.$$

29.—*Desarrollo simbólico de un binomio.*

El notable desarrollo simbólico

$$(a+b)^{\cdot n} = a^{\cdot n} + a^{\cdot n-1} b + a^{\cdot n-2} b^{\cdot 2} + \ldots \qquad (13)$$

es cierto.

Siguiendo en la demostracion de este teorema el método inductivo, supondremos que se verifica para un valor cualquiera n, y probaremos que tambien entónces tiene lugar para el valor $n+1$. Aplicando la forma del número combinatorio de que partimos, tendremos:

$$(a+b)^{\cdot n+1} = \frac{(a+b)(a+b-1)\ldots\ldots (a+b-n)}{1\,.\,2\ldots\ldots (n+1)} = \frac{a+b}{n+1}(a+b-1)^{\cdot n}$$

$$= \frac{a(a+b-1)^{\cdot n} + b(a+b-1)^{\cdot n}}{n+1}.$$

Considerando separadamente cada uno de los términos del numerador del último quebrado, y distribuyendo el trinomio

$$a+b-1$$

en las dos partes

$$(a-1) \quad \text{y} \quad b,$$

segun la hipótesis admitida, el desarrollo del primer término

$$a(a+b-1)^{\cdot n} = a[(a-1)+b]^{\cdot n},$$

será

$$a\left\{(a-1)^{\cdot n} + (a-1)^{\cdot n-1} b + (a-1)^{\cdot n-2} b^{\cdot 2} + \ldots\ldots + b^{\cdot n}\right\};$$

puesto que los términos siguientes (28-2.ª) son nulos.

O bien, efectuando la multiplicacion por a, y teniendo en cuenta el significado de la forma que nos sirve de base, el siguiente:

$$(n+1)\,a^{n+1} + n\,a^{n}\,b + (n-1)\,a^{n-1}\,b^{2} + \ldots\ldots + a\,b^{n}.$$

Cambiando la a en b, por el mismo procedimiento obtendremos para el segundo término

$$b\,(a+b-1)^{n},$$

el desarrollo

$$(n+1)\,b^{n+1} + n\,b^{n}\,a + (n-1)\,b^{n-1}\,a^{2} + \ldots\ldots + b\,a^{n}:$$

el cual, escribiéndolo en orden inverso, y anteponiendo la base a al factor b, se convierte en este otro:

$$a^{n}\,b + 2\,a^{n-1}\,b^{2} + \ldots\ldots + n\,a\,b^{n} + (n+1)\,b^{n+1}.$$

Colocando esta série y la encontrada antes para el primer término, una debajo de otra, de manera que figuren en columna sus términos semejantes respecto de a y b, como sigue,

$$(n+1)\,a^{n+1} + n\,a^{n}\,b + (n-1)\,a^{n-1}\,b^{2} + \ldots\ldots + a\,b^{n}$$

$$a^{n}\,b + 2\,a^{n-1}\,b^{2} + \ldots\ldots + n\,a\,b^{n} + (n+1)\,b^{n}$$

se ve que los coeficientes en una y otra,

$$n+1,\quad n,\quad n-1,\ldots\ldots\quad 1,\quad 0,$$

$$0,\quad 1,\quad 2,\quad \ldots\ldots\quad n,\quad n+1,$$

se corresponden de modo que la suma de cada dos de aquellos es siempre igual á $(n+1)$. Sumando, pues, dichos desarrollos y separando este factor comun en la suma, tendremos al fin:

$$a\,(a+b-1)^{\cdot n} + b\,(a+b-1)^{\cdot n} =$$

$$(n+1)\left\{ a^{\cdot n+1} + a^{\cdot n}\,b + a^{\cdot n-1}\,b^{2} + \ldots\ldots + b^{\cdot n+1} \right\};$$

y la expresion primeramente escrita para la potencia

$$(a+b)^{\cdot n+1}$$

se convierte en esta otra:

$$(a+b)^{\cdot n+1} = a^{\cdot n+1} + a^{\cdot n}\,b + a^{\cdot n-1}\,b^{\cdot 2} + \ldots\ldots + b^{\cdot n+1}$$

Esta igualdad demuestra que si la ley (13) se verifica para un exponente n, tambien es cierta para el inmediato superior, $n+1$. Ahora bien, la mencionada ley tiene lugar para $n=1$, puesto que (28-2.ª) efectivamente es:

$$(a+b)^{\cdot 1} = a^{\cdot 1} + b$$

$$= a^{\cdot 1} + a^{\cdot 1-1}\,b + a^{\cdot 1-2}\,b^{\cdot 2} + \ldots\ldots :$$

luego es cierta para todo valor positivo de n.

Mas tambien, cuando n sea negativo, los dos miembros de la fórmula en cuestion se convierten (28-2.ª) en cero; y, cuando n sea cero, la referida fórmula (13) se transforma en la identidad $1=1$: luego es general para cualquiera valor entero de n.

30.—*Séries binomias.—Definicion.*

La série

$$1 + n\,x + n^{\cdot 2}\,x^{2} + n^{\cdot 3}\,x^{3} + \ldots\ldots$$

se llama *binomia*, x su *base*, y n su *indice*.

No siendo la base $x = 0$, esta série comprende $(n+1)$ términos diferentes de cero, siempre que n sea entero, positivo ó nulo, y el último de ellos es entónces x^n; pero, si n fuese negativo ó fraccionario, dicha série contendría infinitos términos diferentes de cero. Así se desprende de los principios antes demostrados (28); mas conviene advertir aún que, por más que el índice n no tenga igual sentido que la base a en los números combinatorios, le miraremos, sin embargo, en adelante, como entero y positivo exclusivamente.

31.—*Producto de séries binomias.*

El producto de dos ó más séries binomias, de igual base, es otra série binomia de la misma base, y cuyo índice es la suma de los índices de las séries-factores.

En efecto, tomemos primeramente dos séries binomias nada más. Efectuando su producto resultará:

$$(1 + ax + a^{\cdot 2}x^2 + \ldots\ldots)(1 + bx + b^{\cdot 2}x^2 + \ldots\ldots) =$$

$$= 1 + a \left| \begin{array}{l} x + a^{\cdot 2} \\ + b \left| \begin{array}{l} + ab \\ + b^{\cdot 2} \end{array} \right. \end{array} \right| \begin{array}{l} x^2 + \ldots\ldots \\ \\ \\ \\ \\ \\ \\ \end{array} \left| \begin{array}{l} + a^{\cdot r} \\ + a^{\cdot r-1}\, b \\ + a^{\cdot r-2}\, b^{\cdot 2} \\ \vdots \\ \vdots \\ \vdots \\ + b^{\cdot r} \end{array} \right| \begin{array}{l} x^r + \ldots\ldots \\ \\ \\ \\ \\ \\ \\ \end{array}$$

$$= 1 + (a+b)x + (a+b)^{\cdot 2}x^2 + \ldots\ldots + (a+b)^{\cdot r}x^r + \ldots\ldots$$

segun lo demostrado (29).

Ahora bien, si tomásemos várias séries A, B, C..... con los índi-

ces a, b, c..... respectivamente, la série-producto AB, de las dos primeras, tendria por índice $a+b$, segun acabamos de demostrar; mas la série-producto ABC, del producto anterior AB y de la otra série C, por igual razon, tendria por índice

$$a+b+c;$$

y así aconteceria para cualquier número de séries: luego el teorema es general.

32.—*Potencia de una série binomia.*

La potencia entera de una série binomia A, de índice a, es otra série binomia cuyo índice es na.

La proposicion es evidente con sólo advertir que

$$A^n = (\overbrace{A\,A \ldots\ldots A}^{n});$$

y que, segun el teorema anterior, el índice de A^n es

$$(\overbrace{a+a+\ldots\ldots+a}^{n}),$$

ó igual á na.

33.—*Potencia de un binomio.*

Para un exponente real cualquiera, n, se verifica la igualdad

$$(1+x)^n = 1 + nx + n^{\cdot 2}x^2 + \ldots\ldots$$

Concretándonos al caso en que n sea entero y positivo será

$$(1+x)^n = (1 + 1\,.\,x + 1^{\cdot 2}x^2 + \ldots\ldots)^n:$$

puesto que $1^{.2}$, $1^{.3}$..... son cero (28); y, por consecuencia (32),

$$(1+x)^n = 1 + n\,x + n^{.2}\,x^2 + \text{.....}$$

La conocida fórmula del binomio, mediante los símbolos admitidos, puede escribirse del modo siguiente:

$$(a+b)^n = a^n + n\,a^{n-1}\,b + n^{.2}\,a^{n-2}\,b^2 + \text{.....}$$

Para demostrarla basta saber que

$$(a+b)^n = a^n\left(1+\frac{b}{a}\right)^n = a^n\left\{1 + n\,\frac{b}{a} + n^{.2}\,\frac{b^2}{a^2} + \text{.....}\right\};$$

luego, efectuando la multiplicacion indicada, resulta

$$(a+b)^n = a^n + n\,a^{n-1}\,b + n^{.2}\,a^{n-2}\,b^2 + \text{.....}$$

Esta fórmula puede escribirse abreviadamente de este modo:

$$(a+b)^n = \Sigma\, n^{.\alpha}\, a^{n-\alpha}\, b^{\alpha}\,; \qquad (14)$$

en la cual el signo sumatorio comprende todos los valores que toma la expresion á que afecta cuando la letra α recibe sucesivamente los de la série

$$0,\quad 1,\quad 2,\quad 3\text{.....}\quad n.$$

Poniendo $-b$ por b, esta fórmula simbólica se transformará en la siguiente:

$$(a-b)^n = \Sigma\,(-1)^{\alpha}\, n^{.\alpha}\, a^{n-\alpha}\, b^{\alpha}\,;$$

y, suponiendo además que a y b sean iguales á la unidad, aquella y ésta se reducen respectivamente á estas otras:

$$2^n = \Sigma\, n^{.\alpha} \qquad \text{y} \qquad 0 = \Sigma\,(-1)^{\alpha}\, n^{.\alpha}.$$

La segunda de las cuales prueba evidentemente que la suma de los términos de lugar par vale tanto como la de los de lugar impar; y la primera nos manifiesta que cada una de estas sumas es igual á 2^{n-1}.

34.—*Potencia de un polinomio.*

Tomemos ahora un trinomio

$$(a+b+c)$$

y considerémoslo como un binomio cuya primera parte sea $(a+b)$ y la segunda c. Aplicando la fórmula del binomio tendremos:

$$(a+b+c)^n = [(a+b)+c]^n = \Sigma n^{\cdot\gamma} (a+b)^{n-\gamma} c^{\gamma};$$

y, como segun la misma, es

$$(a+b)^{n-\gamma} = \Sigma (n-\gamma)^{\cdot\beta} a^{n-\gamma-\beta} b^{\beta},$$

escribiendo la suma del producto en lugar del producto de las sumas de los factores, será

$$(a+b+c)^n = \Sigma n^{\cdot\gamma} (n-\gamma)^{\cdot\beta} a^{n-\gamma-\beta} b^{\beta} c^{\gamma};$$

ó bien, desarrollando los números combinatorios

$$n^{\cdot\gamma} \quad \text{y} \quad (n-\gamma)^{\cdot\beta},$$

la siguiente:

$$(a+b+c)^n =$$

$$\Sigma \frac{n(n-1)\ldots\ldots (n-\gamma)\ldots\ldots (n-\gamma-\beta+1)}{1.2\ldots\ldots \beta . 1.2\ldots\ldots \gamma} a^{n-\gamma-\beta} b^{\beta} c^{\gamma}$$

$$= \Sigma \frac{n(n-1)\ldots\ldots (n-\alpha+1)}{1.2\ldots\ldots \beta . 1.2\ldots\ldots \gamma} a^{n-\alpha} b^{\beta} c^{\gamma}$$

donde se ha supuesto

$$\beta + \gamma = \alpha.$$

Aplicando este mismo procedimiento al cuatrinomio

$$(a + b + c + d)$$

tendremos:

$$(a+b+c+d)^n = [(a+b+c)+d]^n = \Sigma\, n^{\cdot\delta} (a+b+c)^{n-\delta} d^\delta$$

$$= \frac{n^{\cdot\delta}\,(n-\delta)\,(n-\delta-1).....\,(n-\delta-\gamma-\beta+1)}{1\,.\,2.....\,\beta\,.\,1\,.\,2.....\,\gamma} a^{n-\delta-\gamma-\beta} b^\beta c^\gamma d^\delta$$

$$= \Sigma\, \frac{n(n-1).....\,(n-\alpha+1)}{1\,.\,2.....\,\beta\,.\,1\,.\,2.....\,\gamma\,.\,1\,.\,2.....\,\delta} a^{n-\alpha} b^\beta c^\gamma d^\delta$$

donde se ha supuesto

$$\beta + \gamma + \delta = \alpha.$$

De igual manera se hallará el término sumatorio, general, para un polinomio cualquiera, el cual tendrá por expresion la siguiente:

$$(a+b+c+.....)^n = \Sigma\, \frac{n(n-1).....\,(n-\alpha+1)}{1\,.\,2.....\,\beta\,.\,1\,.\,2.....\,\gamma.....} a^{n-\alpha} b^\beta c^\gamma ..... \quad (15)$$

donde

$$\alpha = \beta + \gamma + \ldots$$

CAPITULO II.

De la Teoria de los Números.—Cómo se consideran y estudian los números en esta parte de la Matemática.

35.—*Ideas generales.*

En el capítulo precedente hemos procurado exponer en breves términos el objeto de la *Aritmética* vulgar, ó propiamente dicha. Resumiendo y ampliando ligeramente ahora las principales ideas ya enunciadas, intentaremos de igual modo definir y caracterizar lo que se entiende y debe entenderse por *Teoría de los Números.*

De lo expuesto en casi todos los párrafos del capítulo anterior se colige que en el concepto de *cantidad* matemáticamente considerada se contienen dos ideas opuestas: una, *abstracta*, que corresponde á la de pura relacion entre los objetos finitos, con formas propias, que para determinar aquella se comparan; y otra, *concreta*, que es la misma de la entidad ú objeto que por tipo de comparacion se hubiere adoptado: el *número* representa la primera, y la *unidad* la segunda.

La cantidad matemática, por consecuencia, el *quantum determinado* que dicen los filósofos, comprende dos ideas y determinaciones muy distintas, que vulgarmente se denominan *discreta* y *contínua;* cada una de las cuales prepondera sobre la otra en las diversas ramas de la Matemática, fundiéndose, por fin, con igual valor, en el *quantum* del *Análisis:* en la cantidad *infinitesimal.*

Es sabido que la determinacion numérica predomina en la Aritmética; pero, si bien el número ó cantidad discreta, que constituye su propio objeto, se nos presenta, en absoluto, como conjunto de unidades idénticas, como resultado de la repeticion ó engendrado por el *uno* constante é indivisible (4), tambien hemos visto que, para la completa realizacion de su concepto, hemos tenido que concretar aquel *uno* generador, calificándolo en unos casos (8), y dotándole en otros de la propie-

dad de dividirse en unidades subalternas de distintos órdenes, como acontece en los quebrados, aunque sujetándose siempre, y con dependencia ineludible, á la unidad fundamental.

De aquí se infiere que, no obstante la supremacía de la *discrecion* en el número, debemos no perder de vista un momento, para darnos cuenta cabal del resultado de las operaciones aritméticas, que su unidad generatriz, ya realmente, ya como ideal, conserva su carácter *contínuo* y concreto: y así se explica que las palabras *número* y *cantidad* se usen muchas veces indistintamente. El problema que, en general, resuelve la Aritmética, consiste en hallar diferentes formas para un mismo número. Estas formas fundamentales son, como sabemos,

$$a + b = c\,, \qquad ab = c\,, \qquad a^n = c\,,$$

que, con la introduccion de los números negativos, fraccionarios, irracionales é imaginarios, comprenden todos los casos posibles, real y efectivamente, ó de un modo formal nada más, y son la base para la natural division de dicha ciencia.

Más ampliamente considerada, abraza tambien la Aritmética la resolucion de los problemas cuyo objeto es convertir unas formas en otras.

Pero tanto en la resolucion del primer problema, como en la del segundo, la *Aritmética propiamente dicha*, como se nota á poco que se reflexione acerca del carácter y verdadera índole de sus operaciones, y sobre el esencial papel que representan los términos que figuran en ellas, se limita á las relaciones puramente externas, digámoslo así, de los números, guardando en sus procedimientos no poca semejanza con la *Geometría*, que tambien se concreta á enseñarnos las relaciones de las magnitudes extensas, pero sin intentar siquiera medirlas en sí mismas, sino puramente compararlas en cuanto respecta á los efectos *totales* de sus dimensiones; y sujetándose en gran parte á la manera como tales números y operaciones se efectúan y representan dentro de un sistema determinado.

La *Teoría de los Números*, ó *Aritmética trascendente*, como algunos (*) la llaman, por el contrario, sin preocuparse para nada de los sis-

(*) *Poinsot.* Réflexions sur les principes fondamentaux, etc., *Schwarz*, etc.

temas de numeracion, estudia los números en sí mismos y sus propiedades permanentes en todos los sistemas posibles; y, sin pararse en esta envoltura superficial, penetra en la íntima constitucion del número, que considera como resultado exclusivamente de la reunion de unidades discretas, cuyos modos de union y enlace examina íntimamente para explicarnos cómo adquiriera aquél su propia y total existencia.

La expresion simbólica, característica, del modo como estas partes discretas se reunen para constituir el todo, se llama *forma numérica.*

Toda forma numérica debe necesariamente componerse de las fundamentales que determina la Aritmética; y es claro que los elementos constituyentes de una cualquiera pueden tambien ser á su vez formas numéricas, subalternas, y abrazar éstas otras inferiores, desempeñando así el papel de individuos constituidos en diferentes órdenes gerárquicos, respecto de la superior inmediata, todas las en ella comprendidas. Mas para que tal gradacion pueda establecerse es preciso que dichas formas contengan dos clases de elementos: *constantes* unos, aunque generales y como indeterminados, que las caracterizen y definan; y otros, *variables* ó *arbitrarios*, de los cuales podremos disponer para que la forma principal represente ciertos números ó formas particulares dadas.

Desde luego se concibe que lo esencial y permanente en toda forma numérica es la ley ó relacion entre sus varios elementos constitutivos: ley de las relaciones y propiedades de dichos elementos, y de las operaciones que con ellos deberán efectuarse para *construir*, mediante una forma dada, las clases y subclases de números y formas subalternas que implícitamente contiene.

Una forma numérica general, por consecuencia, es el compendio de las propiedades comunes á las subalternas, é individuos correspondientes en ella contenidos; y no será difícil, en cierto sentido, deducir las últimas, dada la primera.

Como ejemplos sencillos de tal deduccion presentamos las formas que á continuacion se expresan.

36.—*Números figurados.*

La forma general ó compendiosa de los *números figurados*, de una clase cualquiera n, hallada ya (23) en otra ocasion, es ésta:

$$\frac{a\,(a+1)\ldots\ldots\,(a+n-1)}{1\,.\,2\ldots\ldots\,n}$$

Sus clases subalternas se obtienen dando á n sucesivamente los valores de la série entera 1, 2, 3..... etc., y son las contenidas en el adjunto cuadro.

NÚMEROS FIGURADOS.

Clases.	Sus formas.	Individuos de éstas.	Sus nombres.
1.ª	a	1, 2, 3, 4, 5, 6.....	Naturales.
2.ª	$\frac{a\,(a+1)}{1\,.\,2}$	1, 3, 6, 10, 15.....	Triangulares.
3.ª	$\frac{a\,(a+1)\,(a+2)}{1\,.\,2\,.\,3}$	1, 4, 10, 20, 35.....	Piramidales.
4.ª	$\frac{a\,(a+1)\,(a+2)\,(a+3)}{1\,.\,2\,.\,3\,.\,4}$	1, 5, 15, 35, 70.....	Triángulo-triangulares.
5.ª	$\frac{a\,(a+1)\,(a+2)\,(a+3)\,(a+4)}{1\,.\,2\,.\,3\,.\,4\,.\,5}$	1, 6, 21, 56, 126.....	Triángulo-piramidales.
⋮	⋮	⋮	⋮

Las denominaciones de estos números proceden de que pueden agruparse, formando triángulos, pirámides, etc., tantos objetos (de igual forma, se entiende) como unidades aquellos contengan.

37.—*Números poligonales.*

La forma representativa de los números *poligonales* es como sigue:

$$a + \frac{a(a-1)}{2} n,$$

cuyas clases subalternas é individuos figuran en este cuadro:

NÚMEROS POLIGONALES.

Clases.	Sus formas.	Individuos de éstas.	Sus nombres.
1.ª	$\frac{a(a+1)}{2}$	1, 3, 6, 10, 15, ...	Trigonales.
2.ª	a^2	1, 4, 9, 16, 25, ...	Tetragonales.
3.ª	$\frac{a(3a-1)}{2}$	1, 5, 12, 22, 35, . . .	Pentagonales.
4.ª	$a(2a-1)$	1, 6, 15, 28, 45, . . .	Exagonales.
5.ª	$\frac{a(5a-3)}{2}$	1, 7, 18, 34, 55, . . .	Eptagonales.
⋮	⋮	⋮	⋮

Haciendo, en la forma general, $n = A - 2$, la de los números *Agonales* será finalmente:

$$\frac{(A-2)a^2 - (A-4)a}{2}.$$

Con tantos objetos de igual forma como unidades contienen los números de cada una de las clases comprendidas en el cuadro anterior, se pueden formar los polígonos regulares de donde se derivan sus respectivas denominaciones. Mas conviene saber de antemano cuántos objetos habrá que colocar en fila para formar el lado ó *raiz* del polígono que se trate de construir; y, como consecuencia tambien, algunas de las propiedades que se desprenden de la estructura de los números poligonales.

Supongamos, pues, que N sea un individuo cualquiera de la clase de los trigonales, tendremos:

$$N = \frac{a(a+1)}{2} \quad ;$$

de donde, considerando el lado a como incógnita, se deduce la ecuacion

$$a^2 + a - 2N = 0,$$

cuya solucion entera y positiva es

$$a = \frac{-1+\sqrt{8N+1}}{2}.$$

Ahora bien, para que a sea entero, conforme exige la última igualdad, es necesario que $8N+1$ sea un cuadrado; y de aquí se desprende la propiedad notable de que *el óctuplo de todo número trigonal, sumado con la unidad, produce un cuadrado.* Por igual procedimiento se descubre que los *tetragonales* son cuadrados; que lo son tambien los productos por 24, más la unidad, de los *pentagonales;* que los *exagonales* coinciden con los *trigonales* en la propiedad de que en éstos hicimos mérito; que los *eptagonales* satisfacen á la condicion de ser tambien un cuadrado la forma $40N+9$; los *octagonales* á la de serlo la forma $3N+1$; y, por último, que si N representa, como en los casos ya considerados, un individuo cualquiera de la clase A, sus propiedades están compendiadas en la expresion general

$$\frac{A-4+\sqrt{8(A-2)N+(A-4)^2}}{2(A-2)}.$$

En cuanto á las relaciones de estas especies de números entre sí, y con los términos de la série natural (5), ya indicó Fermat, pero sin demostrarlo, que uno cualquiera de estos términos, a, por ejemplo, multiplicado por el que sigue $(a+1)$, da un producto $a(a+1)$, igual al duplo de su número *triangular* correspondiente, que es, segun hemos visto,

$$\frac{a(a+1)}{2};$$

que el producto del mismo número a por el triangular, correspondiente al superior inmediato $(a+1)$, que es

$$\frac{(a+1)(a+2)}{2},$$

es igual al triplo del *piramidal* del primero a; etc.

Tambien se deduce de la forma conocida de los números *poligonales*

$$a+n\,\frac{(a-1)a}{1.2}=\frac{a(a+1)}{1.2}+(n-1)\,\frac{(a-1)a}{1.2}$$

que representa, como sabemos, el de $A=n+2$ lados iguales á a, que este número poligonal está compuesto de n triangulares: uno de ellos igual á

$$\frac{a(a+1)}{2},$$

cuyo lado es a, y $(n-1)$ iguales á

$$\frac{(a-1)a}{2},$$

cuyo lado es $(a-1)$. Sin demostrarlo tampoco, sentó además Fermat que todo número, ó era trigonal, ó estaba compuesto de dos ó tres números trigonales; que, ó era él mismo cuadrado, ó estaba compuesto por dos, tres ó cuatro cuadrados; pentagonal, ó compuesto por dos, tres, cuatro ó cinco números pentagonales; etc. (*)

(*) *Fermat.* Notes sur Diophante, l. IX.—*Le Besgue.* Introduction à la théorie des nombres.

38.—*Clasificacion de los Números.—Objeto concreto de su Teoría.*

Pero todos estos pormenores curiosos de los ejemplos que hemos examinado, si bien indican el carácter, y el modo como consideramos ahora los números, no penetran en el fondo del asunto tan de lleno como si hubiéramos tomado por objeto de nuestras investigaciones las formas más generales

$$a + bx + cx^2 \quad \text{y} \quad a + bx + cx^2 + dx^3$$

en las que están incluidos no solamente los números *poligonales* y, en cierto modo, los *figurados,* sino otros muchos números además de varias especies.

De esta observacion se desprende que, al estudiar en esta parte de la Matemática los números ó formas numéricas, habremos de preferir aquellas, cuya composicion sea la más general y significativa, y comprenda, por consecuencia, mayor número de formas particulares. Procediendo así, desde lo sencillo á lo complicado, es óbvio que deberemos comenzar por la investigacion de las propiedades más generales tambien de los números, como nos los presenta la Aritmética y ya conocemos, convenientes para agruparlos en el menor número de clases posible, y en las cuales hemos de fundar la institucion de las formas generales á que antes aludimos. Dadas estas formas, no será dificil averiguar despues las relaciones que deban existir entre un número cualquiera y los elementos ya caracterizados que en aquellas figuren, para que dicho número logre ser por las mismas *construido* ó representado; y de esta manera, unas veces ascendiendo desde los números, ó formas individuales, á las genéricas, ya en sentido inverso, descendiendo, llegaremos á plantear y resolver el problema de la *construccion* de los números, que constituye realmente el objeto de nuestra *Teoría.*

A la verdad, el estudio que, segun lo dicho, hemos de emprender desde luego, acerca de las propiedades de los números para clasificarlos, y representarlos así por el menor número de formas posible, debiera di-

rigirse, para ser completo, sobre todas las especies de números definidos al tratar de las operaciones de cálculo, partiendo de la forma comprensiva de todos ellos, de la forma *compleja*, conjunto de los reales é imaginarios, en su total y doble significado, discreto-contínuo; pero, ni la Matemática ha dado solucion cumplida todavía á este problema general, ni las tentativas que para resolverlo han hecho últimamente los más conocidos analistas son de tan escasa importancia que quepan dentro de la índole y extension del presente libro. Términos, pues, de la série numérica (5) son los individuos que comprenden las formas particulares, anteriormente escritas; y sobre los números enteros, mientras expresamente no digamos otra cosa, versarán nuestras inmediatas investigaciones para determinar sus caractéres comunes, esenciales y más fecundos, con el objeto poco antes manifestado.

Desde luego se ocurre que la série entera

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,.....$$

puede dividirse en dos, tres, cuatro, etc., séries subalternas, á saber:

$$\left\{\begin{array}{l} 0,\ 2,\ 4,\ 6,..... \left\{\begin{array}{l} 0,\ 3,\ 6,\ 9,..... \\ 1,\ 4,\ 7,\ 10,..... \\ 2,\ 5,\ 8,\ 11,..... \end{array}\right. \\ 1,\ 3,\ 5,\ 7,..... \left\{\begin{array}{l} 0,\ 4,\ 8,\ 12,..... \\ 1,\ 5,\ 9,\ 13,..... \\ 2,\ 6,\ 10,\ 14,..... \\ 3,\ 7,\ 11,\ 15,..... \end{array}\right. \end{array}\right. \quad \text{etc.}$$

cuyas formas respectivas son:

$$\left\{\begin{array}{l} 2x+0 \\ 2x+1 \end{array}\right. \qquad \left\{\begin{array}{l} 3x+0 \\ 3x+1 \\ 3x+2 \end{array}\right. \qquad \left\{\begin{array}{l} 4x+0 \\ 4x+1 \\ 4x+2 \\ 4x+3 \end{array}\right. \qquad \text{etc.}$$

todas comprendidas en la general

$$kx+r.$$

Examinando estas clasificaciones, se ve que para formarlas hemos

tomado por tipos los números 2, 3, 4..... etc., y los menores que éstos

$$0, 1, \quad 0, 1, 2, \quad 0, 1, 2, 3,$$

respectivamente; y esta observacion nos conduce como por la mano á investigar las propiedades de los números que contengan por factores á los tipos 2, 3, 4..... etc., mencionados, y las de aquellos otros que no los contengan exactamente: en una palabra, las clasificaciones naturales de los términos de la série numérica, que preceden, nos inducen lógicamente á tratar de la *Divisibilidad* y de la *Congruencia* de los números.

CAPITULO III.

De la Divisibilidad de los Números.

39.—*Proposiciones elementales.*

Dícese que un número a es *múltiplo* de otro b, ó que a es *divisible* por b; ó bien que b es *divisor* ó *factor* de a, ó *está contenido* en a; siempre que exista otro número x que verifique la igualdad

$$a = b\,x.$$

De estas definiciones se desprenden las consecuencias siguientes:

1.ª *Todo número está contenido en sí mismo, ó es divisor de sí mismo.* Puesto que, si a es un número cualquiera, tenemos (6)

$$a = 1 \,.\, a.$$

De aquí se deduce además que *la unidad se considera tambien como divisor de todos los números.*

2.ª *Si b se halla contenido β veces en a, y c está contenido γ veces en b, estará c contenido $\beta\gamma$ veces en a;* pues, por hipótesis, tenemos:

$$a = b\beta$$

$$b = c\gamma\,;$$

y sustituyendo este valor de b en la primera igualdad resulta esta otra

$$a = c\beta\gamma = c(\beta\gamma)\,,$$

que demuestra el teorema.

En general, *dada una série de números, cada uno de los cuales sea múltiplo del siguiente, uno cualquiera de ellos es tambien múltiplo de todos los posteriores.*

3.ª *Si b está contenido β veces en a, mb estará tambien contenido en ma igual número β de veces; y la reciproca es cierta.*

En efecto:

1.° Segun la hipótesis, tenemos

$$a = b\beta\,:$$

luego

$$ma = m(b\beta) = mb(\beta)$$

2.° Si mb está contenido β veces en ma, será

$$ma = mb\beta = m(b\beta)\,:$$

de donde resulta:

$$a = b\beta.$$

4.ª *Si dos números a y b son múltiplos de un tercero c, la suma y la diferencia de los dos primeros será tambien múltiplo del tercero.* Puesto que de las igualdades que expresan las hipótesis,

$$a = c\gamma$$

$$b = c\gamma'\,,$$

se deduce esta otra,

$$a \pm b = (\gamma \pm \gamma')c\,.$$

que demuestra la tésis.

40.—*Máximo comun divisor de dos números.*

Todo número, contenido en otros vários, se llama su *divisor comun.*

Problema. Dados dos números a, b, *el primero* a *de los cuales sea igual ó mayor que el segundo* b, *hallar todos sus divisores* D *comunes.*

Dividiendo el número a por el número b, y llamando γ al cociente, y c al resto correspondiente, tendremos la igualdad

$$a = \gamma b + c.$$

Si el resto c fuese cero, el divisor b contendria los divisores comunes de a y b; pero, no siendo c nulo, como los divisores del dividendo a y del divisor b lo son tambien, con mayor motivo, del producto γb, y, por consecuencia (39-4.ª), del resto c, diferencia entre el número a y el mencionado producto γb, resulta que tales divisores, comunes al dividendo a y al divisor b, referidos, coinciden con los de éste último b, y el resto c.

Operando ahora con estos números b y c, del mismo modo que antes lo hicimos con los a y b, hallaremos la segunda igualdad

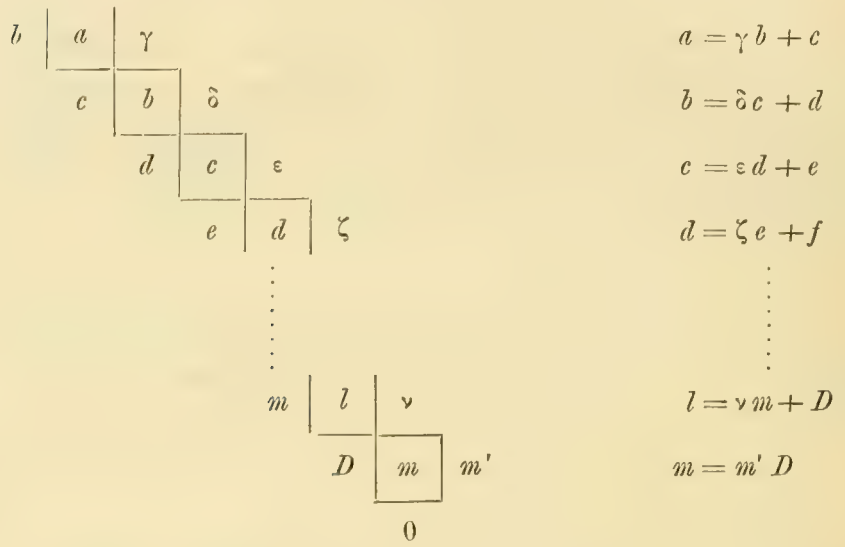
$$b = \delta c + d$$

en la cual δ y d representan el cociente y el resto respectivamente de esta nueva division.

Si en esta segunda igualdad el resto d fuese cero, el divisor c contendria todos los divisores comunes de los números dados a, b; pero, si tampoco d fuese aquí cero, como los divisores de b y c son los mismos que los de c y d, por iguales razones que antes expusimos, dividiríamos nuevamente c por d, y obtendríamos una igualdad semejante á las anteriores acerca de la cual haríamos análogo género de consideraciones.

Así continuaríamos, dividiendo cada vez el divisor por el resto, hasta llegar á un resto cero: lo cual necesariamente debe ocurrir despues de un número finito de divisiones; puesto que los restos sucesivos c, d..... son todos menores que b, y van disminuyendo constantemente. El pro-

cedimiento para resolver el problema propuesto, tal como lo hemos explicado, y las igualdades que de cada division se deducen, figuran en el cuadro siguiente:



Ahora bien, segun el razonamiento en que motivamos las divisiones sucesivas para resolver el problema propuesto, y el modo como se han establecido las anteriores igualdades, es claro que los divisores comunes de los números a y b coinciden con los del penúltimo resto ó último divisor D: y, como este número D es su mayor divisor (39–1.ª), resulta que es tambien el *máximo comun divisor* de los a y b.

La série de igualdades arriba escrita ha sido deducida lógicamente, en el supuesto de ser a *mayor*, ó, por lo menos, *igual* á b. Esta limitacion, sin embargo, desaparece considerando que, en el caso de ser a *menor* que b, tendría que ser $\gamma = 0$, y por consecuencia, $a = c$; y entónces los números b y c estarian sometidos á las condiciones antes exigidas para los a y b. La série de igualdades mencionada se verifica, pues, sin excepcion alguna; como debe suceder para que así podamos dar por terminada la cuestion propuesta.

41.—*Números primos entre sí.—Teorema fundamental.*

Dos números, cuyo máximo comun divisor sea la unidad, se llaman *primos relativos*, *primos entre sí* ó *primos uno con otro.*

Teorema. Si los números a, b, *son primos relativos*, *y* N, *otro número cualquiera*, *todo divisor comun de los números* aN, b, *lo será tambien de los números* N, b.

En efecto, multiplicando por el número N la série de igualdades del párrafo anterior, despues de hacer en la penúltima el máximo comun divisor $D = 1$, obtendremos esta otra série:

$$\begin{aligned} aN &= \gamma\, bN + cN \\ bN &= \delta\, cN + dN \\ cN &= \varepsilon\, dN + eN \\ &\vdots \\ lN &= \nu\, mN + N. \end{aligned}$$

Ahora bien, todo divisor comun D de los números aN, b, lo será de $\gamma\, bN$, y, por consecuencia (39-4.ª), de

$$cN = aN - \gamma\, bN.$$

Siendo D divisor de cN, y por tanto de $\delta\, cN$, como lo es, por hipótesis, de b, y con mayor razon de bN, lo será tambien de

$$dN = bN - \delta\, cN.$$

Prosiguiendo el mismo razonamiento concluiremos que D es divisor necesariamente de lN y $\nu\, mN$, y, por consiguiente, de

$$N = lN - \nu\, mN,$$

que es lo que pretendíamos demostrar.

De este teorema se deducen los corolarios siguientes:

1.° *El producto* aN *de dos números* a, N, *primos ambos con un tercero* b, *es tambien primo con éste.*

Pues, segun el teorema, los números aN y b contienen los mismos divisores que N y b; pero éstos son primos entre sí: luego aN y b lo son tambien.

2.° *Si el producto* aN *es divisible por* b, *y* b *es primo con* a, *debe ser* b *divisor de* N.

Puesto que, segun la hipótesis, b es divisor comun de los números aN y b; y, como es primo con a, conforme al teorema fundamental, será tambien divisor de N.

El primer corolario puede generalizarse de este modo:

3.° *Si varios números*

$$a,\ b,\ c,\ d,\ e,.....$$

son primos con otro α, *el producto de todos los primeros*

$$abcde.....$$

será tambien primo con el segundo α.

O bien, todavía más, diciendo:

Si tenemos dos séries de números

$$a,\ b,\ c,\ d,.....$$

$$\alpha,\ \beta,\ \gamma,\ \delta,.... .$$

tales, que cada término de una de ellas sea primo con cada uno de la otra, el producto de todos los términos de la primera será primo tambien con el producto de todos los términos de la segunda.

Pues, segun el corolario aludido, los productos

$$ab,\quad abc=(ab)c,\quad abcd=(abc)d,$$

y al fin

$$abcde.....$$

son primos con α: del mismo modo se patentiza que el producto

$$abcde.....$$

es primo tambien con β, y con γ, y con δ..... etc., y, por consecuencia, con el producto

$$\alpha\beta\gamma\delta.....$$

4.° Si suponemos ahora que los factores

$$a,\ b,\ c,\ d,.....$$

sean todos iguales al primero a, y los del segundo producto

$$\alpha,\ \beta,\ \gamma,\ \delta.....$$

sean todos iguales al primero tambien α, resultará que

Las potencias enteras de dos números a y α, primos entre sí, serán tambien números primos relativos.

De este principio se deduce el siguiente:

5.° *La raiz m de un número entero A, ó es irracional, ó es tambien un número entero.*

En efecto, supongamos que dicha raiz fuese un quebrado *irreducible* $a:b$, cuyos dos términos son primos entre sí; lo cual puede siempre admitirse. La potencia m de este quebrado, $a^m:b^m$, que, segun acabamos de demostrar, tambien sería irreducible, habría de ser igual al número entero A; pero, como a^m y b^m son primos relativos, a^m no podrá ser divisible por b^m sino en el caso de ser $b^m=1$; y, por consecuencia, $b=1$, y el quebrado supuesto $a:b=a$, número entero. Luego, si la raiz del número A no es entera, tampoco puede ser fraccionaria, y será, por tanto, irracional.

42.—*Máximo comun divisor de varios números.*

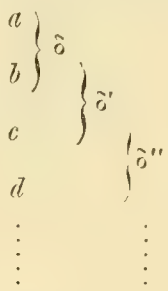
El problema resuelto (40) para dos números solamente, podemos ampliarlo ahora á varios números, y enunciarlo de este modo:

Hallar el máximo comun divisor de varios números.

Sean estos números

$$a,\ b,\ c,\ d.....$$

los cuales, para que se vea bien claro el procedimiento que hemos de explicar, colocaremos del modo siguiente:



en cuyo cuadro representa δ el máximo comun divisor de los dos primeros a, b; δ' el máximo comun divisor del máximo comun divisor δ de los dos primeros, y del tercero c; δ'', de igual manera, el máximo comun divisor de δ', d; etc.

Segun demostramos (40), todos los divisores de los números a, b, están contenidos en su máximo comun divisor δ; luego los divisores comunes de los números a, b, c coinciden con los de los números δ, c; y recíprocamente. Por igual razon los divisores comunes de los números δ, c están todos contenidos en su máximo comun divisor δ'; y, por consecuencia, los divisores comunes de los números a, b, c coinciden con los del número δ'. Del mismo modo se demostraría que los divisores comunes de los números a, b, c, d están contenidos en el número δ''; y, razonando así sucesivamente con todos los números dados,

$$a,\ b,\ c,\ d,\ e.....$$

deduciríamos, por fin, que existe siempre un número, donde se hallan contenidos los divisores comunes de los propuestos; y el cual, obtenido mediante el encadenamiento de operaciones indicado, es realmente el *máximo comun divisor* de todos ellos.

No hay para qué demostrar, despues de lo dicho, que el máximo comun divisor de varios números puede hallarse tambien como indican

las igualdades siguientes que tampoco necesitan, para ser inteligibles, nuevas explicaciones. Designando, pues, por $\delta(d, b, c.....)$ el *máximo comun divisor* de los números $a, b, c.....$, tendremos:

$$\delta(a, b, c) = \delta\{\delta(a, b), c\} = \delta\{\delta(a, c), b\} = \delta\{\delta(b, c), a\}$$

$$\delta(a, b, c, d) = \delta\{\delta(a, b, c), d\} = \delta\{\delta(a, b), \delta(c, d)\} = \text{etc.},$$

cuyas fórmulas pueden extenderse naturalmente á una multitud cualquiera de números.

Los números cuyo máximo comun divisor sea la unidad se llaman, en general, *primos relativos* ó *primos entre sí;* pero, si cada dos cualesquiera de ellos fuesen tambien primos relativos, se denominan especialmente *primos entre sí dos á dos.*

Teorema. Si designamos por δ *un divisor comun de los números* a, b, $c.....$, *y los cocientes enteros,*

$$a : \delta = \alpha, \quad b : \delta = \beta, \quad c : \delta = \gamma.....$$

no son primos entre sí, existe otro divisor comun de los mismos números, múltiplo de δ, *y, por consecuencia, mayor que* δ.

En efecto, por hipótesis tenemos

$$a = \delta\alpha, \quad b = \delta\beta, \quad c = \delta\gamma. \ ...;$$

y, si los cocientes $\alpha, \beta, \gamma.....$ no son primos relativos, contendrán un factor comun $d > 1$, y podremos escribir, por consecuencia, las igualdades,

$$\alpha = d\alpha', \quad \beta = d\beta', \quad \gamma = d\gamma'.....$$

Sustituyendo estos valores de $\alpha, \beta, \gamma.. ..$ en las primeras, resultan estas otras:

$$a = \delta d\alpha', \quad b = \delta d\beta', \quad c = \delta d\gamma'.....;$$

ó bien, haciendo $\delta d = D$, de donde se deduce $D > \delta$ por ser $d > 1$, las siguientes:

$$a = D\alpha', \quad b = D\beta', \quad c = D\gamma'.....$$

que demuestran el teorema.

Corolario. Si los cocientes α, β, γ..... fuesen primos entre sí, no tendrian más factor comun que la unidad; y, por lo tanto, no existiria ningun divisor comun, $D > \delta$, de los números a, b, c.....: es decir, que δ sería entónces el máximo comun divisor de estos números; y recíprocamente: si δ fuese el máximo comun divisor de los números a, b, c..... los cocientes

$$a : \delta = \alpha, \quad b : \delta = \beta, \quad c : \delta = \gamma.....$$

serian primos entre sí.

43.—*Mínimo comun múltiplo de dos números.*

Todo múltiplo de varios números se llama su *múltiplo comun.*

Problema. Hallar todos los dividendos ó múltiplos comunes de dos números.

Sean estos números a, b; y, pues los que buscamos han de ser múltiplos de a, tendrán la forma ma, siendo m entero. Designemos por δ el máximo comun divisor de los dos números a, b, los cuales podrán entónces escribirse bajo las formas

$$\frac{a}{\delta} \cdot \delta \quad \text{y} \quad \frac{b}{\delta} \cdot \delta;$$

y el múltiplo ma, por consecuencia, bajo esta otra:

$$m \frac{a}{\delta} \cdot \delta$$

Pero este múltiplo

$$ma = m \frac{a}{\delta} \cdot \delta$$

debe ser divisible tambien por

$$b = \frac{b}{\delta} \cdot \delta;$$

y, para que ésto sea posible, como

$$\frac{a}{\delta} \quad \text{y} \quad \frac{b}{\delta}$$

son primos entre sí, es necesario (41-2.°) que m sea divisible por $\frac{b}{\delta}$.

Haciendo, pues,

$$m = m' \frac{b}{\delta}$$

(siendo m' entero), y sustituyendo este nuevo valor de m en el múltiplo ma, resultará esta nueva forma,

$$m' \frac{ab}{\delta},$$

para los múltiplos de los números a, b; por cuyos números, como indican las igualdades,

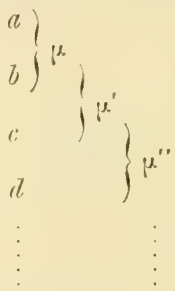
$$m' \frac{ab}{\delta} = m' \frac{b}{\delta} \cdot a = m' \frac{a}{\delta} \cdot b,$$

es aquella en efecto divisible. Luego todos los múltiplos comunes de los dos números a, b, son múltiplos de cierto número, determinado por la forma $\frac{ab}{\delta}$, que representa el *mínimo comun múltiplo* de los dos propuestos. De esta forma se deduce, en lenguaje vulgar, la regla que sigue:

Para hallar el mínimo comun múltiplo de dos números, se multiplica uno de ellos por el cociente que resulte de dividir el otro por el máximo comun divisor de ambos; ó bien, *se divide su producto por este máximo comun divisor.*

44.—*Mínimo comun múltiplo de varios números.*

Razonando ahora como en el problema (42), é indicando de un modo semejante la resolucion del actual, tendremos:



en cuyo cuadro representa μ el mínimo comun múltiplo de los dos números a, b, siendo, por consecuencia,

$$\mu = \frac{a\,b}{\delta};$$

μ' el mínimo comun múltiplo de los números μ, c; μ'' el de los números μ', d; etc. Y así se demuestra sencillamente que los múltiplos comunes de una série de números

$$a,\ b,\ c,\ d.....$$

coinciden con los múltiplos de un solo número, que se llama *mínimo comun múltiplo* de todos ellos, y se obtiene mediante el procedimiento en el adjunto cuadro señalado.

Este mínimo comun múltiplo puede tambien obtenerse, como indican las fórmulas siguientes, análogas á las del máximo comun-divisor:

$$\mu(a, b, c) = \mu\{\mu(a, b), c\} = \mu\{\mu(a, c), b\} = \mu\{\mu(b, c), a\}$$

$$\mu(a, b, c, d) = \mu\{\mu(a, b, c), d\} = \mu\{\mu(a, b), \mu(c, d)\} = \text{etc.}$$

que pueden ampliarse para cualquiera otra multitud de números.

Corolario. Si los números dados

$$a,\ b,\ c,\ d.....$$

fuesen primos entre sí dos á dos, cada par de ellos, tal como a, b, tendría por máximo comun divisor la unidad, y su *mínimo comun múltiplo*, $\frac{ab}{\delta}$, sería simplemente ab; pero c es tambien primo con a y b, y, por consecuencia (41-1.º) con su producto ab; luego el *mínimo comun múltiplo* de los números a, b y c sería abc; y, así razonando, se concluiría que:

El mínimo comun múltiplo de varios números, primos entre sí dos á dos, es el producto de todos ellos.

De esta proposicion se deduce esta otra:

Todo número, divisible por otros varios, primos entre sí dos á dos, es tambien divisible por el producto de todos ellos.

Teorema. Si designamos por μ *un múltiplo comun de los números* a, b, $c.....$, *y los cocientes enteros*,

$$\mu : a = \alpha,\quad \mu : b = \beta,\quad \mu : c = \gamma.....$$

no son primos entre sí, existe otro múltiplo comun de los mismos números, divisor de μ, *y, por consecuencia, menor que* μ.

En efecto, por hipótesis tenemos:

$$\mu = a\alpha = b\beta = c\gamma = ... ;$$

y, si los cocientes α, β, $\gamma.....$ no son primos relativos, tendrán un factor comun $m > 1$, y podremos escribir, por consecuencia, las igualdades

$$\alpha = m\alpha',\quad \beta = m\beta',\quad \gamma = m\gamma'.....$$

Sustituyendo estos valores de α, β, $\gamma.....$ en las primeras, se obtendrán estas otras:

$$\mu = am\alpha' = bm\beta' = cm\gamma' = ... ;$$

ó bien, haciendo $\mu = m M$, de donde se deduce $M < \mu$ por ser $m > 1$, las siguientes:

$$M = a\alpha' = b\beta' = c\gamma' = \ldots\ldots$$

que demuestran el teorema.

Corolario. Si los cocientes α, β, γ..... fuesen primos entre sí, no tendrían más factor comun que la unidad, y, por lo tanto, sería

$$m = 1 \quad \text{y} \quad \mu = M:$$

esto es, no existiría ningun múltiplo M de los números dados menor que μ. Y recíprocamente, si μ fuese el *mínimo comun múltiplo* de los números a, b, c .... los cocientes α, β, γ..... serían primos entre sí.

45.—*Números primos absolutos.*

Dijimos (39), que todo número es divisible por sí mismo y por la unidad.

Tratándose de la unidad estos dos divisores coinciden y se reducen á uno solo. Prescindiendo, pues, de este factor necesario y general de todos los números, llamaremos *primo absoluto* ó sencillamente *primo*, y tambien *simple*, al número que no sea divisible sino por sí mismo y por la unidad.

De esta definicion se deduce, que el máximo comun divisor de un número cualquiera y otro número primo, sólo puede ser este número primo ó la unidad; luego

Todo número primo que no sea divisor de otros números cualesquiera es primo con cada uno de ellos, y por consecuencia (41–3.°) *con su producto.* De donde:

Para que un número primo sea divisor de un producto de varios factores, es necesario que divida á alguno de estos factores.

46.—*Números compuestos.—Teorema fundamental.*

Todo número que, además de sí mismo y de la unidad, contenga algun otro divisor, se llama *compuesto*.

Teorema. Todo número compuesto es siempre el producto de un número finito de factores primos.

En efecto: sea N un número compuesto, el cual, segun la definicion, contendrá al divisor a. Si este divisor a no es primo, contendrá á su vez otro divisor b; si tampoco fuese b primo, contendrá otro divisor c: y continuando del mismo modo, como los divisores $a, b, c.....$ son menores que N y van disminuyendo, por precision tendremos que llegar á un número primo, único caso en que la série de los divisores a, b, $c.....$ no podría ya prolongarse.

Sea, pues, p este número primo en que termina la série mencionada: desde luego podremos escribir sin inconveniente la igualdad

$$N = p\,N'.$$

Ahora bien, si el número N' fuese primo, el teorema estaria demostrado; pero, si fuese compuesto, buscaríamos, como antes para N, un divisor suyo primo. Designando por p' este nuevo divisor, podremos escribir la igualdad

$$N' = p'\,N'',$$

y, por consecuencia, esta otra:

$$N = pp'\,N''.$$

Razonando, respecto de este nuevo número N'', como lo hemos hecho respecto del N', y prosiguiendo así, hallaremos, por fin, que el número propuesto N es efectivamente un producto finito de factores primos, y puede expresarse por la forma

$$N = pp'p''.....$$

Hemos demostrado la posibilidad de descomponer un número compuesto en factores primos; pero falta demostrar ahora que tal descomposicion puede efectuarse de un *solo* modo, ó lo que es igual, que

Dos productos de factores primos no pueden ser iguales, si los factores del primero no son respectivamente iguales á los del segundo.

Supongamos para ésto que se verifique la igualdad de los dos productos

$$a\,b\,c\ldots\ldots = a'\,b'\,c'\ldots\ldots$$

Puesto que el segundo producto es divisible evidentemente por a', deberá serlo tambien el primero; y por tanto, es necesario que un factor cualquiera de éste, a, por ejemplo, sea divisible por a': pero a es primo y no contiene, por consecuencia, otros divisores sino él mismo y la unidad: luego para que a sea divisible por a', es necesario que sean iguales, esto es, $a = a'$. Del mismo modo que hemos demostrado la igualdad de estos dos factores, podríamos demostrar la de los restantes, y probar la exactitud del teorema enunciado. Mas conviene advertir que en el razonamiento empleado en esta demostracion, no hemos tenido en cuenta para nada que los factores primos de cada producto entren en ellos una sola vez ó se hallen varias veces repetidos; por cuya razon podemos afirmar en definitiva, que:

Para ser iguales dos números compuestos es necesario que consten de los mismos factores primos, y además que cada factor esté contenido en ellos igual número de veces.

En conformidad con este principio, la forma general de todo número compuesto puede expresarse como sigue:

$$N = a^{\alpha}\ b^{\beta}\ c^{\gamma}\ldots\ldots$$

donde a, b, c..... designan números primos absolutos, y los exponentes α, β, γ..... el número de veces respectivamente que cada uno de aquellos se halla, como factor, en N repetido.

Aunque la forma anterior la hemos deducido en la hipótesis de ser N un número compuesto, nótese, sin embargo, que tambien comprende á los números primos.

47.—*Forma de los divisores de un número.*

El número

$$N = a^{\alpha}\ b^{\beta}\ c^{\gamma}\ .....$$

no será divisible por $a^{\alpha'}$ *cuando sea* $\alpha' > \alpha$.

En efecto, hagamos

$$\alpha' = \alpha + r,$$

en cuyo caso será

$$a^{\alpha'} = a^{\alpha} \cdot a^{r}$$

Dividiendo por esta igualdad la anterior, tendremos:

$$N : a^{\alpha'} = b^{\beta}\ c^{\gamma}\ ..... : a^{r},$$

y, como los factores b, c..... son primos con a, el cociente

$$b^{\beta}\ c^{\gamma}\ ..... : a^{r}$$

no puede ser entero: esto es, N no puede ser divisible por $a^{\alpha'}$.

Segun lo dicho, para que un número

$$N = a^{\alpha}\ b^{\beta}\ c^{\gamma}\ .....$$

sea divisible por otro

$$d = a^{\alpha'}\ b^{\beta'}\ c^{\gamma'}\ ....,$$

es necesario que los factores inclusos en éste no sean diferentes de los contenidos en el primero, y además que los exponentes que figuran en el divisor representen:

α'	uno cualquiera de los	$(\alpha+1)$	números	$0, 1, 2..... \alpha,$
β'		$(\beta+1)$		$0, 1, 2..... \beta,$
γ'		$(\gamma+1)$		$0, 1, 2..... \gamma,$
.....				

Tal es el criterio tambien para conocer si un número es divisible por otro.

48.—*Multitud de todos los divisores de un número.*

Todos los números d, resultantes de dar á los exponentes $\alpha', \beta', \gamma'.....$ los valores que acabamos de expresar, son efectivamente divisores del número N. Las séries de estos divisores, por consecuencia, que producen respectivamente los factores primos de N, son

$$1, a, a^2 .. .. a^\alpha$$
$$1, b, b^2 ..... b^\beta$$
$$1, c, c^2 ..... c^\gamma$$
$$.....$$

y, como cada combinacion de un valor de α' con otro de β', con otro de $\gamma'.....$ etc., constituye un divisor tambien de N, pero diferente de los que resulten de otra combinacion cualquiera, es claro que el número de todos los divisores de N, la unidad y este mismo número inclusive, es igual al de todas las combinaciones posibles, de todas clases, que pueden formarse con los términos de las séries anteriores. Este número, incluyendo la unidad como divisor, sabemos (27) tiene por expresion el producto

$$(\alpha+1)(\beta+1)(\gamma+1).....$$

que es independiente de la naturaleza de los factores de N.

49.—*Suma de todos los divisores de un número.*

Los diferentes divisores del número N se hallarán, segun hemos indicado, multiplicando sucesivamente cada uno de los términos de las séries correspondientes á sus factores primos, antes escritas, por todos los términos restantes; obteniendo así con estos términos productos de la forma

$$a^{\alpha'} b^{\beta'} c^{\gamma'} \ldots\ldots$$

De un modo semejante se obtendrá la suma de todos los divisores del número N: multiplicando entre sí las sumas parciales de todos los divisores contenidos en cada una de las séries mencionadas. Pero estas sumas parciales son las siguientes:

$$1 + a + a^2 + \ldots\ldots + a^{\alpha} = \frac{a^{\alpha+1} - 1}{a - 1}$$

$$1 + b + b^2 + \ldots\ldots + b^{\beta} = \frac{b^{\beta+1} - 1}{b - 1}$$

$$1 + c + c^2 + \ldots\ldots + c^{\gamma} = \frac{c^{\gamma+1} - 1}{c - 1}$$

Luego la suma de todos los divisores del número N será:

$$\frac{a^{\alpha+1} - 1}{a - 1} \cdot \frac{b^{\beta+1} - 1}{b - 1} \cdot \frac{c^{\gamma+1} - 1}{c - 1} \ldots\ldots$$

Ejemplo. Dado

$$N = 252000 = 2^5 . 3^2 . 5^3 . 7$$

el número de todos los divisores de este número será:

$$(5+1)(2+1)(3+1)(1+1) = 6.3.4.2 = 144.$$

y la suma de estos mismos divisores

$$\frac{2^6-1}{2-1} \cdot \frac{3^3-1}{3-1} \cdot \frac{5^4-1}{5-1} \cdot \frac{7^2-1}{7-1} = 63.13.156.8 = 367012.$$

50.—*Determinacion del máximo comun divisor y mínimo comun múltiplo de varios números mediante sus factores primos.*

La descomposicion de los números en sus factores primos absolutos nos proporciona un medio sencillo de resolver nuevamente los problemas resueltos ya de otro modo (42) y (44), y en este epígrafe enunciados.

En efecto, segun las definiciones correspondientes (40) y (43), y el criterio establecido (47) de la divisibilidad de un número por otro, descompuestos varios números A, B, C..... en sus factores primos, su *máximo comun divisor* será el producto de las menores potencias de cada uno de estos factores primos que sean comunes á los números dados; y su *mínimo comun múltiplo* será el producto de todos los factores primos que figuren en las respectivas descomposiciones de los números propuestos, pero entrando en dicho producto las mayores potencias de cada uno de aquellos factores primos.

Es evidente que si los factores primos del número A, son todos diferentes de los del número B, y los de B diferentes de los de C, etc., no existirá ningun factor *comun* á los números dados A, B, C..... cuyo *máximo comun divisor* será entónces la unidad.

Sean los números

$$A = 504, \quad B = 2880, \quad C = 864.$$

Descomponiendo estos números en sus factores primos tendremos las igualdades:

$$504 = 2^3.3^2.7, \qquad 2880 = 2^6.3^2.5, \qquad 864 = 2^5.3^3.$$

Los factores comunes á los tres números dados son 2 y 3, y los exponentes menores de cada uno de estos factores comunes son 3 y 2: luego el máximo comun divisor que se busca será el producto

$$2^3 . 3^2 = 72.$$

Todos los factores primos que figuran en las descomposiciones de los números propuestos son

$$2, \quad 3, \quad 5, \quad 7;$$

y sus mayores potencias

$$2^6, \quad 3^3, \quad 5, \quad 7:$$

luego el mínimo comun múltiplo de los números dados será el producto

$$2^6 . 3^3 . 5 . 7 = 60480.$$

La descomposicion en factores simples sirve tambien para conocer si un número es potencia de otro. Así, dado un número

$$N = a^\alpha \, b^\beta \, c^\gamma \ldots\ldots,$$

para que sea una potencia K^n, por ejemplo, de otro número K, es necesario que los exponentes, α, β, γ..... de los factores del primero sean divisibles por el de la potencia, n, del segundo, pues este número K no puede contener factores diferentes de los contenidos en N; y, si K contiene α' veces al factor a, la potencia $N = K^n$ lo contendrá $n\alpha'$ veces: luego será $n\alpha' = \alpha$, y, por consecuencia, α divisible por n; pudiéndose demostrar lo mismo de los exponentes de los otros factores.

51.—*Ley de Euler.*

De la expresion general (49) se desprende que lo primero que conviene hacer para hallar la suma de todos los divisores de un número (la unidad y el mismo número inclusive) es descomponerlo en sus factores primos. Así formó *Euler* la tabla siguiente, donde al lado de cada uno de los 100 primeros números, figuran los que expresan las sumas de todos sus divisores.

1	1	21	32	41	42	61	62	81	121
2	3	22	36	42	96	62	96	82	126
3	4	23	24	43	44	63	104	83	84
4	7	24	60	44	84	64	127	84	224
5	6	25	31	45	78	65	84	85	108
6	12	26	42	46	72	66	144	86	132
7	8	27	40	47	48	67	68	87	120
8	15	28	56	48	124	68	126	88	180
9	13	29	30	49	57	69	96	89	90
10	18	30	72	50	93	70	144	90	234
11	12	31	32	51	72	71	72	91	112
12	28	32	63	52	98	72	195	92	168
13	14	33	48	53	54	73	74	93	128
14	24	34	54	54	120	74	114	94	144
15	24	35	48	55	72	75	124	95	120
16	31	36	91	56	120	76	140	96	252
17	18	37	38	57	80	77	96	97	98
18	39	38	60	58	90	78	168	98	171
19	20	39	56	59	60	79	80	99	156
20	42	40	90	60	168	80	186	100	217

«Si contemplamos, dice *Euler* (*), la série de los números

$$1,\ 3,\ 4,\ 7,\ 6,\ 12.....$$

que representan las sumas de todos los divisores de los términos de la série aritmética, ninguna ley parece vislumbrarse entre ellos; empero, meditándolo despacio, he descubierto que la série en cuestion obedece á una ley constante, segun la cual uno cualquiera de sus términos puede ser formado por algunos términos precedentes.»

Representando por $S(N)$ la suma de los divisores de N, la ley de *Euler* se halla expresada en la igualdad siguiente:

$$\begin{aligned} S(N) = {} & S(N-1) + S(N-2) - S(N-5) - S(N-7) \\ & + S(N-12) + S(N-15) - S(N-22) - S(N-26) \\ & + S(N-35) + S(N-40) - S(N-51) - S(N-57) \\ & + S(N-70) + S(N-77) - S(N-92) - S(N-100) + \cdots\cdots \end{aligned}$$

Aunque esta série pueda prolongarse indefinidamente, se tomarán de ella, en cada caso, los términos desde el principio hasta el primero que resulte negativo exclusive; teniendo además en cuenta que, si al aplicarla se encontrase el término $S(0)$, en lugar de este valor indeterminado, debe siempre ponerse el mismo número N.

Dividiendo la série para $S(N)$ en dos, de modo que comiencen respectivamente por los dos primeros términos positivos, y vayan alternando luego en ellas los signos $+$ y $-$; y fijándose en los sustraendos solamente que figuran en cada una de ellas, esto es, en los números

$$1,\ 5,\ 12,\ 22,\ 35,\ 51.....$$

para la primera, y en los

$$2,\ 7,\ 15,\ 26,\ 40,\ 57.....$$

para la segunda, se halla facilmente que la forma del término general

(*) Commentationes arithmeticæ, t. I, pág. 147, y t. II, pág. 105 y 639.

de ambas es

$$\frac{3a^2-a}{2} = \frac{a(3a-1)}{2} :$$

la misma que representa los números *pentagonales* (37). Esta forma, para valores positivos de a, dará los términos de la primera série de sustraendos, y los de la segunda para valores negativos del mismo a. Dando, pues, al número a sucesivamente los valores 0, 1, 2..... y los valores 0, -1, -2..... la série resultante de números pentagonales, prolongada naturalmente por la derecha y por la izquierda, será ésta:

.....77, 57, 40, 26, 15, 7, 2, 0, 1, 5, 12, 22, 35, 51.....

Finalmente, ordenando estos números segun sus valores absolutos, tendremos la série de sustraendos

0, 1, 2, 5, 7, 12, 15, 22, 26, 35, 40, 51.....

que figuran en la fórmula de *Euler*.

Este célebre matemático confiesa ingénuamente que no encontró la demostracion rigurosa de tal ley; pero el camino que para definirla ó enunciarla siguiera, con escasas variantes, es el que á continuacion trascribimos.

Al producto infinito

$$s = (1+a)(1+b)(1+c)(1+d).....$$

puede dársele la forma siguiente:

$$s = (1+a)+b(1+a)+c(1+a)(1+b)+d(1+a)(1+b)(1+c)+\cdots\cdots :$$

y, haciendo

$$a = -x, \quad b = -x^2, \quad c = -x^3, \quad d = -x^1, \ldots\ldots$$

esta otra:

$$s = 1-x-x^2(1-x)-x^3(1-x)(1-x^2)-x^4(1-x)(1-x^2)(1-x^3)-\cdots\cdots$$

Establezcamos ahora por analogía las igualdades

$$s' = 1-x+x(1-x)(1-x^2)+x^2(1-x)(1-x^2)(1-x^3)+\cdots\cdots$$

$$s'' = 1-x^2+x^2(1-x^2)(1-x^3)+x^4(1-x^2)(1-x^3)(1-x^4)+\cdots\cdots$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$s^{(n)} = 1-x^n+x^n(1-x^n)(1-x^{n+1})+x^{2n}(1-x^n)(1-x^{n+1})(1-x^{n+2})+\cdots\cdots$$

$$s^{(n+1)} = 1-x^{n+1}+x^{n+1}(1-x^{n+1})(1-x^{n+2})+x^{2n+2}(1-x^{n+1})(1-x^{n+2})(1-x^{n+3})+\cdots\cdots$$

Separando el factor $(1-x^n)$ en la série $s^{(n)}$, resulta la que sigue:

$$s^{(n)} = \left\{1+x^n(1-x^{n+1})+x^{2n}(1-x^{n+1})(1-x^{n+2})+\cdots\cdots\right\}(1-x^n)$$

Efectuando esta multiplicacion y ordenando respecto de x, será el producto

$$s^{(n)} = 1+x^n(1-x^{n+1})+x^{2n}(1-x^{n+1})(1-x^{n+2})+\cdots\cdots$$

$$-x^n\cdots\cdots\cdots-x^{2n}(1-x^{n+1})\cdots\cdots\cdots-\cdots\cdots$$

y, despues de sencillas reducciones,

$$s^{(n)} = 1-x^{2n+1}-x^{3n+2}(1-x^{n+1})-x^{4n+3}(1-x^{n+1})(1-x^{n+2})-\cdots\cdots$$

ó finalmente:

$$s^{(n)} = 1-x^{2n+1}-x^{3n+2}\left\{1-x^{n+1}+x^{n+1}(1-x^{n+1})(1-x^{n+2})+\cdots\cdots\right\}$$

Ahora bien, si reparamos que la série inclusa en este paréntesis es la correspondiente á $s^{(n+1)}$ antes escrita, podemos establecer la fórmula general

$$s^{(n)} = 1-x^{2n+1}-x^{3n+2}s^{(n+1)}$$

que comprenderá todas las anteriores, si convenimos en que para $n=0$ sea $s^{(0)}=s$. Esto supuesto, tendremos para los valores de

$$n=0,\quad 1,\quad 2,\quad 3,\quad 4.....$$

los de las séries correspondientes, como á continuacion figuran:

$$\begin{array}{ll} n=0 & s = 1-x-x^2 s' \\ n=1 & s' = 1-x^3-x^5 s'' \\ n=2 & s'' = 1-x^5-x^8 s''' \\ n=3 & s''' = 1-x^7-x^{11} s^{IV} \\ n=4 & s^{IV} = 1-x^9-x^{11} s^{V} \\ \cdots\cdots & \cdots\cdots\cdots\cdots \\ \cdots\cdots & \cdots\cdots\cdots\cdots\cdots \end{array}$$

Sustituyendo por

$$s',\quad s'',\quad s''',\quad s^{IV}.....$$

sus valores respectivos, la série s tomará la forma

$$s = 1-x-x^2(1-x^3)+x^{2+5}(1-x^5)-x^{2+5+8}(1-x^7)$$
$$+x^{2+5+8+11}(1-x^9)-.....$$

ó, efectuando las operaciones indicadas, esta otra:

$$s = 1-x-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+x^{26}-x^{35}-.....$$

cuyos exponentes constituyen la série de los números *pentagonales*.

Tomemos ahora logaritmos del primer producto s, y tendremos:

$$\text{L. } s = \text{L. }(1-x)+\text{L. }(1-x^2)+\text{L. }(1-x^3)+.....$$

Aplicando á cada uno de los términos de este segundo miembro el conocido desarrollo

$$\text{L.}\,(1-y) = -y - \frac{y^2}{2} - \frac{y^3}{3} - \frac{y^4}{4} - \cdots\cdots$$

y sumando y ordenando las séries resultantes, se obtiene la siguiente:

$$\begin{aligned}
-\text{L.}\,s = x &+ \frac{x^2}{2} + \frac{x^3}{3} + \frac{x^4}{4} + \frac{x^5}{5} + \frac{x^6}{6} + \frac{x^7}{7} + \frac{x^8}{8} + \frac{x^9}{9} + \cdots\cdots \\
&+ \frac{x^2}{1} \quad + \frac{x^4}{2} \quad + \frac{x^6}{3} \quad + \frac{x^8}{4} \quad + \cdots\cdots \\
&+ \frac{x^3}{1} \quad + \frac{x^6}{2} \quad + \frac{x^9}{3} + \cdots\cdots \\
&+ \frac{x^4}{1} \quad + \frac{x^8}{2} \quad + \cdots\cdots \\
&+ \frac{x^5}{1} \\
&+ \frac{x^6}{1} \\
&+ \frac{x^7}{1} \\
&+ \frac{x^8}{1} \\
&+ \frac{x^9}{1} + \cdots\cdots
\end{aligned}$$

A poco que en este cuadro se repare, se advertirá que los exponentes de x en la primera fila son los números naturales; los exponentes de x en la segunda fila son los múltiplos sucesivos de 2; los exponentes de x

en la tercera, los múltiplos sucesivos de 3; y así de las demás: deduciéndose, por consecuencia, la segunda fila de la primera, sustituyendo en ésta por x la potencia segunda x^2; la tercera tambien de la primera, sustituyendo en ésta por x la tercera potencia x^3, etc. Y, en cuanto á las columnas, se notará que los coeficientes de cada una de las potencias de x son quebrados cuyo numerador comun es la unidad, y cuyos denominadores sucesivos son todos los divisores de los respectivos exponentes de las potencias mencionadas.

Así, por ejemplo, los coeficientes de x^4 son los quebrados

$$\frac{1}{1}, \quad \frac{1}{2}, \quad \frac{1}{4};$$

los de x^5 son los quebrados

$$\frac{1}{1}, \quad \frac{1}{5}; \quad \text{etc.}$$

De aquí se sigue que el coeficiente total de x^n tendrá la forma

$$\frac{1}{1} + \frac{1}{d'} + \frac{1}{d''} + \frac{1}{d'''} + \cdots\cdots + \frac{1}{n},$$

representando

$$1, \quad d', \quad d'', \quad d''' \ldots\ldots \quad n$$

todos los divisores de n (la unidad y n inclusive).

Algo más breve y satisfactoriamente puede determinarse la forma general de los coeficientes de x^n en el desarrollo de $\mathrm{L}.s$, por este otro camino, distinto del anterior. Designemos por d un divisor cualquiera del exponente n de x. Es evidente que el término $\frac{x^d}{d}$ se halla comprendido en la fila primera del cuadro anterior; y que entre los desarrollos de

$$\mathrm{L}.(1-x), \quad \mathrm{L}.(1-x^2), \ldots\ldots$$

se hallará el de

$$\mathrm{L}.\left(1-x^{\frac{n}{d}}\right)$$

que debe contener la potencia $\frac{n}{d}$ de x, y tambien el término

$$\frac{\left(\frac{n}{x^d}\right)^d}{d} = \frac{x^n}{d} .$$

Y como d representa un divisor cualquiera de n, y lo que de uno se ha dicho puede repetirse á propósito de los demás, resulta que en la suma de los desarrollos mencionados, la potencia x^n se encontrará dividida por todos estos divisores, en otros tantos distintos términos del desarrollo total.

Si el coeficiente de x^n así deducido, le reducimos á un comun denominador, se transformará en el siguiente:

$$\frac{n + \cdots + d'' + d' + 1}{n} ,$$

que podrá simbólicamente escribirse de este modo:

$$\frac{S(n)}{n} ;$$

y el desarrollo anterior de $-\mathrm{L}.\, s$ como sigue:

$$-\mathrm{L}.\, s = \frac{x}{1} S(1) + \frac{x^2}{2} S(2) + \frac{x^3}{3} S(3) + \frac{x^4}{4} S(4) + \frac{x^5}{5} S(5) + \cdots$$

Diferenciando esta ecuacion (teniendo en cuenta que la variable independiente es x y los logaritmos neperianos) y multiplicando el resultado por x, tendremos:

$$-\frac{x\, d\, s}{s\, d\, x} = x S(1) + x^2 S(2) + x^3 S(3) + x^4 S(4) + x^5 S(5) + \cdots$$

Diferenciando tambien la ecuacion

$$s = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \cdots$$

resulta;

$$\frac{ds}{dx} = -1 - 2x + 5x^4 + 7x^6 - 12x^{11} - 15x^{14} + \cdots$$

y multiplicando ordenadamente este coeficiente diferencial por la igualdad

$$\frac{x}{s} = \frac{x}{1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \cdots},$$

se obtiene la siguiente:

$$-\frac{x\,ds}{s\,dx} = \frac{x + 2x^2 - 5x^5 - 7x^7 + 12x^{12} + 15x^{15} - \cdots}{1 - x - x^2 + x^5 + x^7 - \cdots}$$

De las dos expresiones para

$$-\frac{x\,ds}{s\,dx}$$

se deduce la ecuacion:

$$x + 2x^2 - 5x^5 - 7x^7 + 12x^{12} + 15x^{15} - \cdots$$

$$= \left\{ xS(1) + x^2 S(2) + \cdots \right\} \left\{ 1 - x - x^2 + x^5 + \cdots \right\};$$

y de ésta, efectuando la multiplicacion indicada en su segundo miembro, la que á continuacion se escribe:

$$x + 2x^2 - 5x^5 - 7x^7 + 12x^{12} + 15x^{15} - 22x^{22} - 26x^{26} + \cdots =$$

$$xS(1) + x^2 S(2) + x^3 S(3) + x^4 S(4) + x^5 S(5) + x^6 S(6) + x^7 S(7) + x^8 S(8) + \cdots$$

$$- x^2 S(1) - x^3 S(2) - x^4 S(3) - x^5 S(4) - x^6 S(5) - x^7 S(6) - x^8 S(7) - \cdots$$

$$- x^3 S(1) - x^4 S(2) - x^5 S(3) - x^6 S(4) - x^7 S(5) - x^8 S(7) - \cdots$$

$$+ x^6 S(1) + x^7 S(2) + x^8 S(3) + \cdots$$

$$+ x^8 S(1) + \cdots$$

Comparando ahora los coeficientes de las potencias del mismo grado de x en ambos miembros, resultan las igualdades:

$$1 = S(1) \qquad 0 = S(3) - S(2) - S(1)$$

$$2 = S(2) - S(1) \qquad 0 = S(4) - S(3) - S(2$$

$$-5 = S(5) - S(4) - S(3) \qquad 0 = S(6) - S(5) - S(4) + S(1)$$

$$-7 = S(7) - S(6) - S(5) + S(2) \qquad 0 = S(8) - S(7) - S(6 + S(3) + S(1)$$

. . . . . .

. . . . . .

de las que facilmente se induce que la expresion general que comprende todos estos casos es por fin:

$$S(N) - S(N-1) - S(N-2) + S(N-5) + S(N-7) - \ldots\ldots \pm S(0) = 0,$$

admitiendo, como al principio dijimos, que por $\pm S(0)$ se ponga el valor $\pm N$.

52.—*Números amigables.*

Repetidas veces hemos indicado anteriormente, que entre los divisores de un número compuesto comprendíamos este mismo número y la unidad.

Los divisores de un número, excepto el mismo número, se llaman *partes alicuotas*.

Dos números se denominan *amigables* (*amicabiles*) cuando la suma de las partes alicuotas de uno de ellos es igual al otro.

Así, por ejemplo, los números 220 y 284 son amigables, porque la suma

$$1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284$$

de las partes alicuotas del primero, 220, es igual al segundo, 284; y la

suma de las partes alicuotas de 284, á saber:

$$1 + 2 + 4 + 71 + 142 = 220$$

es igual á 220.

La cuestion actual para nosotros, dentro de la índole de los principios que venimos desenvolviendo, es averiguar si estos números poseen formas generales; ó, al ménos, si, fundados en las propiedades que los caracterizan, podremos instituir algunas formas que, en ciertos casos, los representen.

Siguiendo á *Euler* en estas investigaciones, designemos por a, b dos números *amigables*, y por A, B respectivamente las sumas de todos sus divisores: segun la definicion de tales números tendremos las igualdades:

$$A - a = b, \quad B - b = a$$

de donde se deducen estas otras

$$A = B = a + b.$$

Supongamos que sean

$$a = px, \quad b = qy.$$

siendo x é y primos: y designemos por P y Q, respectivamente tambien, las sumas de todos los divisores de p y q; tendremos (49):

$$A = P(x+1), \quad B = Q(y+1):$$

ó, segun la última igualdad,

$$P(x+1) = Q(y+1) = px + qy.$$

Si hacemos ahora

$$P(x+1) = Q(y+1) = PQz,$$

en cuyo supuesto serán

$$x + 1 = Qz, \quad y + 1 = Pz$$

y tambien, por consecuencia,

$$x = Qz - 1\,, \quad y = Pz - 1\,,$$

llegaremos á la ecuacion

$$z = \frac{p+q}{Qp + Pq - PQ}\,;$$

y, sustituyendo este valor de z, á las siguientes:

$$x + 1 = \frac{Q(p+q)}{Qp + Pq - PQ}\,, \quad y + 1 = \frac{P(p+q)}{Qp + Pq - PQ}$$

que expresan las condiciones para que px y qy sean números amigables.

Representando por δ el máximo comun divisor de los números px y qy, y estableciendo las igualdades

$$p = \delta m\,, \quad q = \delta n\,,$$

y, de consiguiente,

$$P = \Delta M\,, \quad Q = \Delta N\,,$$

las formas de los números amigables serian

$$\delta m x\,, \quad \delta n y\,:$$

en las cuales x, y deben ser números primos que satisfagan á las ecuaciones

$$x + 1 = \frac{\delta B(m+n)}{N\delta m + M\delta n - \Delta MN}\,, \quad y + 1 = \frac{\delta A(m+n)}{N\delta m + M\delta n - \Delta MN}$$

Es bien patente la dificultad de encontrar por tanteo, una vez determinados arbitrariamente m y n, valores convenientes de δ para que los números x, y adquieran por las últimas fórmulas, no sólo valores enteros sino además primos; y, aunque este trabajo pudiera simplificarse, en parte, mediante una tabla que contuviera las sumas de los divisores de los números primos y de sus potencias hasta uno muy elevado, siempre sería, sin embargo, muy embarazosa la aplicacion de las

ecuaciones arriba escritas. No por su utilidad práctica é inmediata, sino por el modo de instituirlas, y el espíritu que á su investigacion preside, conviene, sin embargo, fijar la atencion en estas fórmulas.

53.—*Números perfectos.*

Un número se llama *perfecto*, cuando es igual á la suma de sus partes alicuotas.

Conservando para las letras mayúsculas la misma significacion que les dimos en el párrafo anterior, si designamos por a un número perfecto, será $a = A - a$, y por tanto, $A = 2a$: ley principal de tales números.

Para deducir de esta esencial propiedad, segun hicimos tratándose de los amigables, una forma general de los números perfectos, procederemos de la manera siguiente.

Un número perfecto, a, será *par* ó *impar*. Siendo par, contendrá una potencia cualquiera de 2, y podremos representarlo por la forma $2^n b$, y entónces tendremos (49), y segun la ley antes escrita,

$$A = (2^{n+1} - 1) B = 2^{n+1} b ;$$

de donde se deduce:

$$\frac{B}{b} = \frac{2^{n+1}}{2^{n+1} - 1} .$$

Ahora bien, como el numerador y el denominador de este quebrado numérico son primos entre sí, puesto que se diferencian en la unidad, dicho quebrado es irreducible; y, por consecuencia, los dos términos del primer miembro de la última igualdad serán iguales respectivamente ó equimúltiplos de los del segundo; luego tendremos:

$$b = 2^{n+1} - 1$$

ó bien

$$b = (2^{n+1} - 1) c ,$$

siendo c entero.

En el primer caso, ó sea cuando

$$b = 2^{n+1} - 1,$$

debe verificarse tambien la igualdad entre los numeradores de los dos miembros de la que venimos examinando, es decir:

$$B = 2^{n+1},$$

y para ésto es indispensable que

$$b = 2^{n+1} - 1$$

sea número primo; porque sólo entónces la suma de sus divisores es

$$B = S(b) = S(2^{n+1} - 1) = 2^{n+1};$$

y, por consecuencia, la de sus partes alicuotas es 1; de donde resulta finalmente que, cuando

$$b = 2^{n+1} - 1$$

sea número primo, la forma

$$2^n b = 2^n (2^{n+1} - 1)$$

representará números *perfectos*.

En el segundo caso, á saber:

$$b = (2^{n+1} - 1)c,$$

las partes alicuotas de b serían

$$2^{n+1} - 1 \quad \text{y} \quad c,$$

y la suma $B = S(b)$ no sería menor que

$$2^{n+1} + c + b;$$

de donde se infiere que el quebrado $\frac{B}{b}$ no podría ser menor que

$$2^{n+1} + \frac{c+b}{b} = \frac{2^{n+1}(1+c)}{(2^{n+1}-1)c};$$

pero este último quebrado es mayor que $\frac{B}{b}$; luego no puede admitirse el caso de que sea

$$b = (2^{n+1}-1)c.$$

Conclúyese, por fin, que todos los números perfectos, *pares*, se hallan contenidos en la forma

$$a = 2^n(2^{n+1}-1),$$

siempre que

$$(2^{n+1}-1)$$

represente un número primo.

Para aplicar esta forma daremos á n valores numéricos sucesivos, y veremos, en cada una de estas sustituciones, si

$$2^{n+1}-1$$

es efectivamente número primo. Así, por ejemplo, hallamos que para $n=1$ es

$$2^{n+1}-1 = 3,$$

número primo; y, por tanto,

$$a = 6 = 1+2+3,$$

número perfecto; para $n=2$ es

$$2^{n+1}-1 = 7,$$

número primo; y

$$a = 28 = 1+2+4+7+14;$$

para $n=4$ es

$$2^{n+1}-1 = 31.$$

número primo; y

$$a = 496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248;$$

para $n = 6$ es

$$2^{n+1} - 1 = 127,$$

número primo; y, por consecuencia, $a = 8128$; etc.

La cuestion de si existen ó no, además de los dichos, números perfectos, *impares*, no se ha resuelto científicamente todavía.

54.—*Máxima potencia de un número primo contenida en el producto* $n!$

Reanudando ahora el hilo de nuestras investigaciones sobre la divisibilidad de los números, resolveremos el siguiente problema.

Hallar el exponente de la máxima potencia de un número primo p, *contenida en el producto*

$$n! = 1 . 2 . 3 . 4 ..... n.$$

Designando por n' el entero del cociente completo $\frac{n}{p}$, que tambien se expresa por $\left[\frac{n}{p}\right]$, los factores múltiplos de p, contenidos en el producto $n!$, serán

$$p,\ 2p,\ 3p ..... n'p;$$

y, como para nuestro objeto los restantes factores de $n!$ nada significan, tendremos que averiguar únicamente cuál es la máxima potencia de p contenida en el producto

$$p \times 2p \times 3p \times ..... \times n'p = 1 . 2 . 3 ..... n' . p^{n'}.$$

Procediendo con el producto

$$1 . 2 . 3 ..... n' = n'!$$

del mismo modo que con el $n!$, y llamando n'' al entero $\left[\frac{n'}{p}\right]$, consideraremos el nuevo producto, análogo al anterior,

$$p \times 2p \times 3p \times \ldots\ldots \times n''p = 1 \,.\, 2 \,.\, 3 \ldots\ldots \; n'' p^{n''} .$$

Continuando el mismo procedimiento, puesto que los enteros máximos n', n''..... contenidos respectivamente en los quebrados

$$\frac{n}{p}, \quad \frac{n'}{p} \ldots\ldots$$

van disminuyendo, y su número es finito, por precision habremos de llegar á uno, por ejemplo, $n''' < p$, en cuyo caso será el cociente entero

$$\left[\frac{n'''}{p}\right] = 0.$$

De donde resulta que la potencia máxima de p contenida en $n!$ será entónces

$$p^{n' + n'' + n'''}$$

cuyo exponente es la suma

$$n' + n'' + n''' .$$

Sean, por ejemplo,

$$n = 40, \quad p = 3.$$

Tendremos:

$$n' = \left[\frac{40}{3}\right] = 13; \quad n'' = \left[\frac{13}{3}\right] = 4, \quad n''' = \left[\frac{4}{3}\right] = 1 < 3:$$

luego el exponente de la máxima potencia de 3, contenida en el producto

$$1 \,.\, 2 \,.\, 3 \,.\, 4 \ldots\ldots 40,$$

será

$$13 + 4 + 1 = 18.$$

Nótese que los cocientes enteros

$$n',\ n'',\ n'''.....$$

son los mismos que estos otros:

$$\left[\frac{n}{p}\right],\ \left[\frac{n}{p^2}\right],\ \left[\frac{n}{p^3}\right].....;$$

y tambien que, si fuese n' el cociente entero $\frac{n}{a}$, y n'' el cociente entero $\frac{n'}{b}$, sería n'' el cociente entero $\frac{n}{ab}$. Refiriéndonos al ejemplo anterior, vemos efectivamente que

$$n''=\left[\frac{13}{3}\right]=\left[\frac{40}{3^2}\right]=4;\quad n'''=\left[\frac{4}{3}\right]=\left[\frac{40}{3^3}\right]=1$$

Corolario. El producto

$$1.2.3.....\ m=m!$$

será divisible por el producto

$$1.2.....\ n\times 1.2.....\ p\times 1.2.....\ q\times.....\ =n!\times p!\times q!.....$$

si se verifica la igualdad

$$m=n+p+q+.....$$

En efecto, sea π un factor primo cualquiera del divisor

$$n!\times p!\times q!.....;$$

y designemos por

$$m',\ n',\ p',\ q'.....$$

respectivamente los cocientes enteros

$$\left[\frac{m}{\pi}\right],\ \left[\frac{n}{\pi}\right],\ \left[\frac{p}{\pi}\right],\ \left[\frac{q}{\pi}\right].....$$

Evidentemente tendremos la relacion

$$m' \geqq n' + p' + q' + \cdots\cdots$$

Dividiendo de nuevo por π estos cocientes, y representando por

$$m'', \ n'', \ p'', \ q'' \cdots\cdots$$

los cocientes enteros

$$\left[\frac{m'}{\pi}\right], \ \left[\frac{n'}{\pi}\right], \ \left[\frac{p'}{\pi}\right], \ \left[\frac{q'}{\pi}\right] \cdots\cdots$$

respectivamente, tendremos tambien la relacion

$$m'' \geqq n'' + p'' + q'' + \cdots\cdots$$

Continuando del mismo modo hasta que todos los cocientes enteros sean menores que π, y sumando ordenadamente las relaciones halladas, se obtendrá la siguiente:

$$m' + m'' + m''' + \cdots\cdots \geqq n' + n'' + n''' + \cdots\cdots + p' + p'' + p''' + \cdots\cdots$$
$$+ q' + q'' + q''' + \cdots\cdots$$

Pero estas sumas expresan respectivamente los exponentes de las máximas potencias de π contenidas en el dividendo $m!$ y en el divisor $n! \ p! \ q! \cdots\cdots$: luego no existirá en este divisor ningun factor primo con un exponente superior al que tenga el mismo factor en el dividendo; y, por tanto, el cociente completo

$$\frac{m!}{n! \ p! \ q! \cdots\cdots}$$

será entero.

De este corolario se deduce que *el producto de n números enteros consecutivos*,

$$(m+1)(m+2)(m+3)\cdots\cdots (m+n),$$

es siempre divisible por el de los n primeros números de la série natural,

$$1 \,.\, 2 \,.\, 3 \ldots\ldots \; n\,;$$

pues, multiplicando por el producto

$$1 \,.\, 2 \,.\, 3 \ldots\ldots \; m\,,$$

los dos enunciados, tendremos estos otros:

$$1 \,.\, 2 \,.\, 3 \ldots\ldots \; m \times (m+1)(m+2)(m+3) \ldots\ldots \; (m+n)\,,$$

$$1 \,.\, 2 \,.\, 3 \ldots\ldots \; m \times 1 \,.\, 2 \,.\, 3 \ldots\ldots \; n.$$

Segun el corolario demostrado, como el último factor $(m+n)$ del producto total primero, es la suma de los dos últimos factores, m y n, de los parciales del segundo, el cociente completo

$$\frac{(m+n)\,!}{m\,!\;n\,!}$$

será entero; y, por consecuencia, lo será tambien su igual, expresado por los signos ordinarios algebráicos,

$$\frac{(m+1)(m+2)\ldots}{1 \,.\, 2 \,.\, 3 \ldots\ldots} \cdot \frac{\ldots \; (m+n)}{n}\,.$$

55.—*De los números primos con otro dado é inferiores á éste.*

Problema de suma trascendencia para nuestras ulteriores investigaciones es el que nos proponemos resolver en este párrafo, á saber:

Hallar cuántos números primos con N *existen en la série natural*

$$1\,,\;\; 2\,,\;\; 3\,,\;\; 4 \ldots\ldots \; N.$$

Designando por a, b, c..... los factores primos relativos, de N, distintos de la unidad, es evidente que la cuestion se reduce á indagar

cuántos términos quedarán en la série propuesta,

$$1,\ 2,\ 3,\ 4,\ \ldots\ldots\ N \qquad (N)$$

despues de separar todos los que sean divisibles por los factores mencionados.

Ahora bien, los términos de la série (N) divisibles por a son

$$a,\ 2a,\ 3a\ldots\ldots\ \frac{N}{a}a.$$

cuyo número es $\frac{N}{a}$. Quitando, pues, estos $\frac{N}{a}$ términos de los N de la série dada (N), restan en ella

$$N' = N - \frac{N}{a} = N\left(1 - \frac{1}{a}\right) \qquad (1)$$

términos que no son divisibles por a.

Veremos ahora cuáles son los múltiplos de b, en la série (N) contenidos, y que no han sido ya descontados en el concepto de múltiplos tambien de a. Múltiplos de b contiene aquella série los siguientes:

$$b,\ 2b,\ 3b\ldots\ldots\ \frac{N}{b}b;$$

mas, por ser a y b primos entre sí, los múltiplos de b que tambien lo sean de a deberán hallarse contenidos en esta otra série:

$$1,\ 2,\ 3\ldots\ldots\ \frac{N}{b};$$

y ascenderán, en suma, á $\frac{N}{ba}$. Resulta, pues, que de la série (N), efectuada la supresion de todos los múltiplos de a, sólo habrá que suprimir, en el concepto exclusivo de múltiplos de b, estos términos:

$$\frac{N}{b} - \frac{N}{ab} = \frac{N}{b}\left(1 - \frac{1}{a}\right).$$

En la citada série, hechas ambas supresiones con relacion á los dos factores a y b, quedan todavía los siguientes términos:

$$N'' = N - \frac{N}{a} - \frac{N}{b}\left(1 - \frac{1}{a}\right) = N\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right).$$

Suprimamos ahora los múltiplos de c. En la série primitiva estos múltiplos son los que á renglon seguido figuran:

$$c,\ 2c,\ 3c, \ldots\ldots\ \frac{N}{c}\,c.$$

Los que entre ellos sean múltiplos de a ó de b, y se hayan ya suprimido ó descontado por este motivo, deben buscarse en esta otra série,

$$1,\ 2,\ 3\ldots\ldots\ \frac{N}{c};$$

análoga á la primitiva y que contendrá

$$\frac{N}{c}\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)$$

términos no divisibles por a ni por b, conforme lo acabado de exponer: estos serán precisamente los múltiplos de c que deberemos suprimir para encontrar los términos de la série (N), independientes de los tres factores a, b, y c, hasta ahora considerados. Resulta, pues:

$$N''' = N - \frac{N}{a} - \frac{N}{b}\left(1 - \frac{1}{a}\right) - \frac{N}{c}\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right) =$$

$$N\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\left(1 - \frac{1}{c}\right).$$

Y aplicando el mismo razonamiento al caso de cuatro, cinco, ó más factores del número N, nos resultará para expresion (*) general, $\varphi(N)$,

(*) Gauss.—Disquisitiones arithmeticæ, §. 38.

del total de números primos con N é inferiores á él, la siguiente:

$$\varphi(N) = N\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\cdots\cdots\left(1-\frac{1}{s}\right).$$

Si damos al número N la forma (46)

$$N = a^{\alpha}\, b^{\beta}\, c^{\gamma}\,\ldots\ldots .$$

la funcion $\varphi(N)$ tomará la siguiente:

$$\varphi(N) = (a-1)\,a^{\alpha-1}\,.\,(b-1)\,b^{\beta-1}\,.\,(c-1)\,c^{\gamma-1}\,\ldots\ldots ;$$

ó esta otra:

$$\varphi(N) = N\frac{a-1}{a}\cdot\frac{b-1}{b}\cdot\frac{c-1}{c}\cdots\cdots = \frac{N}{abc\ldots\ldots}(a-1)(b-1)(c-1)\ldots\ldots$$

Escolio. Si fuese N igual á un número primo, p, evidentemente sería

$$\varphi(p) = p-1 ;$$

y, si fuese N igual á una potencia cualquiera p^{π} de un número primo p, aplicando la fórmula general tendríamos:

$$\varphi(p^{\pi}) = (p-1)\,p^{\pi-1} .$$

Si entre los números inferiores y primos con N existe el número α, existirá tambien el $N-\alpha$: luego, hallados los números menores que la mitad del propuesto, N, los restantes serán complementarios de aquellos. Del mismo modo, si N es par, entre los números inferiores y primos con él se hallarán estos dos:

$$\frac{1}{2}N-\alpha \quad \text{y} \quad \frac{1}{2}N+\alpha ;$$

y, si N fuese divisible por un número cualquiera, n, los números

primos con N tambien se hallarían entre los siguientes:

$$\frac{1}{n}N \pm \alpha, \quad \frac{2}{n}N \pm \alpha, \quad \frac{3}{n}N \pm \alpha \ldots\ldots \frac{n-1}{n}N \pm \alpha, \quad N - \alpha.$$

Por último, la expresion general de $\varphi(N)$ patentiza que dicha funcion es siempre un número par, exceptuando los dos casos en que sea

$$N = 1, \quad \text{y} \quad N = 2.$$

Ejemplo. Sea

$$N = 60 = 2^2 . 3 . 5.$$

Tendremos

$$\varphi(60) = 60 . \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = \frac{60}{30} \cdot 1 . 2 . 4 = 16.$$

Y, en efecto, los números primos con 60 de la série

$$1, \ 2, \ 3, \ 4 \ldots\ldots \ 60.$$

son los 16 siguientes:

1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59.

56.—*Demostracion de la ley* $\varphi(NN') = \varphi(N)\varphi(N')$, *cuando* N *y* N' *son primos entre sí.*

De la expresion hallada para la funcion φ se deduce este importante

Teorema. Si los números N *y* N' *son primos entre sí, se verificará la igualdad*

$$\varphi(NN') = \varphi(N)\varphi(N').$$

En efecto, si los números N y N' son primos entre sí, los factores primos absolutos $a, b, c \ldots\ldots$ del primero serán todos diferentes de

los factores primos absolutos, a', b', c'....., del segundo; y, como en el producto de ambos, NN', no puede existir ningun factor primo absoluto, diferente de los factores contenidos en cada uno de ellos, será:

$$\varphi(NN') = NN' \begin{cases} \left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)..... \\ \left(1-\frac{1}{a'}\right)\left(1-\frac{1}{b'}\right)\left(1-\frac{1}{c'}\right)..... \end{cases}$$

Pero tambien tenemos:

$$\varphi(N) = N\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right).....$$

y

$$\varphi(N') = N'\left(1-\frac{1}{a'}\right)\left(1-\frac{1}{b'}\right)\left(1-\frac{1}{c'}\right).....;$$

luego la ley

$$\varphi(NN') = \varphi(N)\varphi(N'),$$

es cierta.

Apoyándose en lo acabado de demostrar, fácilmente se probaría tambien que la ley se verifica cuando son tres los factores considerados; y, en general, para un número cualquiera de números primos entre sí.

Si designamos, pues, por p, q, r..... los factores primos relativos del número N, tendremos:

$$\varphi(N) = \varphi(p)\varphi(q)\varphi(r).....$$

Corolarios. 1.° Si los dos factores en que se descompusiere el número N fuesen los dos inseparables de todo número (excepto la unidad), á saber: el mismo número, y el *uno*, tendríamos:

$$\varphi(N) = \varphi(1)\varphi(N);$$

de cuya igualdad se desprende que es necesario hacer ó suponer

$$\varphi(1) = 1.$$

Ahora bien, entendiendo que la $\varphi(N)$ comprenda los números primos con N y *no mayores* que N, segun exige el valor de $\varphi(1)$ antes establecido, no existirá ya para tal funcion excepcion ninguna.

2.° Si fuese $N = 2p$, siendo p impar y, por tanto, primo con 2, tendríamos tambien

$$\varphi(N) = \varphi(2)\varphi(p) :$$

y, como $\varphi(2) = 1$, será

$$\varphi(2p) = \varphi(p) :$$

es decir, que no existen en la série natural, aritmética, más números primos, y no mayores que el duplo de un número impar, que cuantos haya primos y no mayores que este impar mismo.

57.—*Demostracion de la ley* $\Sigma\varphi(d) = N$, *en la cual* d *representa todos los divisores del número* N.

Determinada la significacion del símbolo $\varphi(N)$ del modo que acabamos de manifestar (55), demostraremos ahora una propiedad del mismo, de grande importancia por sus aplicaciones en lo sucesivo, á saber:

Todo número N *es igual á la suma de los valores de la funcion* φ *sucesivamente aplicada á todos los divisores, primos y compuestos, de dicho número.*

Para ésto recordemos que cualquier divisor d del número

$$N = a^{\alpha}\, b^{\beta}\, c^{\gamma} \ldots\ldots$$

tiene la forma

$$d = a^{\alpha'}\, b^{\beta'}\, c^{\gamma'} \ldots\ldots :$$

y como, por ser $a, b, c \ldots\ldots$ números primos diferentes, sus potencias

$$a^{\alpha'},\ b^{\beta'},\ c^{\gamma'} \ldots\ldots$$

son tambien números primos entre sí, tendremos la expresion (56):

$$\varphi(d) = \varphi(a^{\alpha'})\,\varphi(b^{\beta'})\,\varphi(c^{\gamma'}).....;$$

en la cual α', β'..... pueden tomar todos los valores desde 0 hasta α, desde 0 hasta β..... etc. respectivamente.

El símbolo $\varphi(d)$, equivalente al producto de los símbolos análogos en el segundo miembro de esta igualdad contenidos, puede considerarse como expresion general de un término cualquiera del producto de las siguientes séries:

$$\varphi(1) + \varphi(a) + \varphi(a^2) + \cdots + \varphi(a^{\alpha})$$

$$\varphi(1) + \varphi(b) + \varphi(b^2) + \cdots + \varphi(b^{\beta})$$

$$\varphi(1) + \varphi(c) + \varphi(c^2) + \cdots + \varphi(c^{\gamma})$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

Mas la primera de estas séries, en términos explícitos (55), equivale á la siguiente:

$$1 + (a-1) + (a-1)a + (a-1)a^2 + \cdots + (a-1)a^{\alpha-1},$$

ó bien á esta otra:

$$1 + (a-1)\left\{1 + a + a^2 + \cdots + a^{\alpha-1}\right\} = 1 + (a-1)\frac{a^{\alpha}-1}{a-1} = a^{\alpha};$$

y una cosa semejante podría decirse de las demás.

Luego el producto de todas ellas, ó la suma de los términos que de la expresion $\varphi(d)$ se derivan, podrá representarse de este modo:

$$\Sigma\,\varphi(d) = a^{\alpha}\,b^{\beta}\,c^{\gamma}.....;$$

ó igual al número propuesto N.

Ejemplo. Sea

$$N = 60 = 2^2 . 3 . 5.$$

Las sumas de las progresiones correspondientes á sus factores son:

$$1 + 2 + 4$$
$$1 + 3$$
$$1 + 5$$

El producto de estas progresiones es:

$$1 + 2 + 4 + 3 + 6 + 12 + 5 + 10 + 20 + 15 + 30 + 60.$$

Las séries de la funcion φ correspondientes á las progresiones anteriores son:

$$\varphi(1) + \varphi(2) + \varphi(4) = 1 + 1 + 2 = 4$$
$$\varphi(1) + \varphi(3) = 1 + 2 = 3$$
$$\varphi(1) + \varphi(5) = 1 + 4 = 5$$

cuyo producto es:

$$\varphi(1) + \varphi(2) + \varphi(4) + \varphi(3) + \varphi(2)\varphi(3) + \varphi(4)\varphi(3) + \varphi(5) + \varphi(2)\varphi(5)$$
$$+ \varphi(4)\varphi(5) + \varphi(3)\varphi(5) + \varphi(2)\varphi(3)\varphi(5) + \varphi(4)\varphi(3)\varphi(5);$$

ó bien, en guarismos, este otro:

$$1 + 1 + 2 + 2 + 2 + 4 + 4 + 4 + 8 + 8 + 8 + 16 = 60.$$

Cada término de esta suma es el valor de la φ de cada uno de los términos del producto anterior de las progresiones correspondientes á los factores primos del número 60, cuyo producto comprende todos los divisores de este número. La suma de los valores de la funcion φ aplicada á estos divisores es, efectivamente, el número 60; y el producto

de las sumas de los valores de tal funcion, aplicada á cada uno de los términos de las progresiones correspondientes á los factores primos de 60, es tambien 60.

58.—*Nueva deduccion de la funcion* φ.

La simple condicion que expresa la igualdad

$$\Sigma \varphi(d) = N,$$

en la cual d representa sucesivamente todos los divisores del número N, caracteriza y puede servir para determinar la funcion φ, antes (55) por otro método encontrada.

Pero, como tal determinacion es un corolario de otra proposicion más general, comenzaremos por estudiarla para deducir despues aquella, y otras no ménos interesantes consecuencias.

Sea

$$N = a^{\alpha} b^{\beta} c^{\gamma} \ldots\ldots = a^{\alpha-1} b^{\beta-1} c^{\gamma-1} \ldots\ldots \times a b c \ldots\ldots = N' \times P.$$

La expresion (desarrollada)

$$(a-1)(b-1)(c-1)\ldots\ldots$$

comprende todos los divisores simples y compuestos de P, mitad precedidos del signo $+$, y del $-$ otra mitad. Si representamos, pues, por d_1 uno cualquiera de los divisores positivos, y por d_2 otro cualquiera de los negativos, podremos escribir esta igualdad:

$$(a-1)(b-1)(c-1)\ldots\ldots = \Sigma d_1 - \Sigma d_2. \qquad (1)$$

Y si por d designamos un divisor cualquiera de P, distinto ó inferior á P, vamos á demostrar que en el grupo Σd_1 existirán tantos términos divisibles por d como el Σd_2.

La cosa es evidente cuando $P = a b$, porque entónces

$$\Sigma d_{1-2} - \Sigma d_{2-2} = (a\,b + 1) - (a + b).$$

Si $P = a\,b\,c$,

$$\Sigma d_{1-3} - \Sigma d_{2-3} = (\Sigma d_{1-2} - \Sigma d_{2-2})(c - 1) =$$

$$(c\,\Sigma d_{1-2} + \Sigma d_{2-2}) - (c\,\Sigma d_{2-2} + \Sigma d_{1-2}).$$

Ahora bien, si d divide á varios términos del grupo Σd_{1-3} los dividirá, ó por pertenecer al grupo Σd_{2-2} ó al $c\,\Sigma d_{1-2}$; pero en el grupo Σd_{2-2} existen los mismos términos divisibles por d que en el Σd_{1-2}, segun hemos visto; y los mismos, por consecuencia, existirán en el $c\,\Sigma d_{1-2}$ que en el $c\,\Sigma d_{2-2}$: luego tambien en el caso que ahora consideramos la proposicion es evidente. Y, como el razonamiento es aplicable sin modificacion á todos los casos sucesivos, podemos dar por demostrado el teorema en general.

Consideremos ahora no el número P, compuesto de factores primos, distintos, elevados á la primera potencia, sino el

$$N = a^{\alpha}\,b^{\beta}\,c^{\gamma}\,\ldots\ldots = N'\,P,$$

y formemos esta otra expresion analítica, análoga á la (1), poco antes estudiada:

$$a^{\alpha-1}\,b^{\beta-1}\,c^{\gamma-1}\,\ldots\ldots\,(a-1)(b-1)(c-1)\ldots\ldots =$$

$$N\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\ldots\ldots = \Sigma D_1 - \Sigma D_2 \qquad (2)$$

en la cual los grupos de términos ΣD_1 y ΣD_2 no comprenderán todos los divisores de N, á diferencia de los grupos anteriores Σd_1 y Σd_2 que comprendian todos los divisores de P, sino solamente los divisores de N que resultan de multiplicar los de P por N'. Designando, pues, por D_1 y D_2 dos términos cualesquiera de los grupos ΣD_1 y ΣD_2, en los Σd_1 y Σd_2 existirán otros dos términos cor-

respondientes, y entre unos y otros mediarán estas relaciones necesarias:

$$D_1 = N' d_1 \qquad D_2 = N' d_2 .$$

Si representamos ahora por D un divisor cualquiera de N, inferior á N, fácil nos será demostrar que existen en el grupo ΣD_1 tantos términos divisibles por D como en el ΣD_2.

Para ello designemos por δ el máximo comun divisor de D y N': desde luego podremos escribir estas tres igualdades:

$$D = D' \delta ; \quad N' = N'' \delta ; \quad \text{y} \quad N = P N'' \delta .$$

Puesto que, por hipótesis, D divide á N dividirá $D' \delta$ á $P N'' \delta$, ó bien D' á $P N''$; pero, como D' y N'' son primos entre sí, ésto pide que D' sea divisor de P: por lo tanto, D' en nada se diferencia de lo que antes designamos por d, y así tendremos:

$$D = d \delta .$$

Sea D_1 un número cualquiera del grupo ΣD_1. Para que

$$D_1 = N' d_1$$

sea divisible por D forzosamente ha de ser d_1 divisible por d: luego las condiciones de divisibilidad de los términos comprendidos en ΣD_1 y ΣD_2 por D, son las mismas que las de los términos representados por Σd_1 y Σd_2 por d. En el grupo ΣD_1 habrá, pues, tantos términos divisibles por D como en el ΣD_2.

De esta propiedad de los números D_1 y D_2 se deducen varias importantes consecuencias.

1.ª Supongamos que dos funciones F y f, de forma indeterminada ó desconocida, satisfagan á esta condicion:

$$F(N) = \Sigma f(D) ; \qquad (3)$$

en la cual por N representamos un número cualquiera, y por D todos sus divisores simples y compuestos.

Entre estos divisores, elijamos, y separémoslos en dos grupos distintos, los que antes designamos por los símbolos D_1 y D_2: al primero de los cuales pertenece el mismo número propuesto N.

Si á todos estos números, D_1 y D_2, aplicamos sucesivamente la igualdad (3), y efectuamos despues la suma de las igualdades que corresponden al primer grupo, y luego la de aquellas que se refieren al segundo, ambas sumas sólo pueden discrepar por la $f(N)$ que figura entre los términos de la primera y no entre los de la segunda. Por lo tanto, será en símbolos:

$$f(N) = \Sigma F(D_1) - \Sigma f(D_2) \qquad (4)$$

igualdad, en cierto modo inversa de la anterior (*).

(*) Esto, que es casi evidente, para el lector poco familiarizado con la notacion demasiado general del texto, tal vez presente alguna dificultad. Desmenucémoslo para disiparla por completo.

Por

$$D_1', \quad D_1'', \quad D_1''' \ldots\ldots \quad N,$$

representemos los diversos términos del grupo ΣD_1. Y por

$$D_2', \quad D_2'', \quad D_2''' \ldots\ldots;$$

los comprendidos en el ΣD_2. Por definicion, ó en virtud de la igualdad (3) aplicable á todos estos números, tenemos:

$F(D_1') =$ á la suma de las funciones f, extensivas á todos los divisores de D_1'

$F(D_1'') =$ á id. extensivas á todos los divisores de D_1''

. . . . . .

. . . . . .

Y sumando ordenadamente las anteriores igualdades:

$$F\ D_1') + F_1 D_1'') + \ldots\ldots = \Sigma F(D_1) =$$

á la suma de las funciones f, extensivas á todos los divisores de los términos comprendidos en el grupo ΣD_1, y entre ellos al número propuesto N.

Pero:

$$F_1 D_2') + F(D_2'' + \ldots\ldots = \Sigma F(D_2 =$$

Como aplicacion de esta igualdad supongamos en la (3) que

$$F(N) = N = \Sigma f(D).$$

La (4) se convierte entónces en esta otra:

$$f(N) = \Sigma D_1 - \Sigma D_2$$

ó, recordando el significado y equivalencia (2) del segundo miembro, en ésta:

$$f(N) = N\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\left(1 - \frac{1}{c}\right)\cdots\cdots$$

de donde resulta que, si

$$N = \Sigma f(D), \quad \text{ó} \quad \Sigma \varphi(D),$$

la funcion φ queda determinada por la relacion anterior. Precisamente lo inverso fué lo demostrado y conseguido páginas más atrás (57).

2.ª Si entre las funciones F y f establecemos ahora, en vez de la relacion (3), esta otra,

$$F(N) = \Pi f(D), \tag{5}$$

en la cual N representa un número cualquiera, y Π es inicial de *producto*, extensivo á la funcion f de todos los divisores D, de N, concluiremos tambien, mediante un razonamiento análogo al que minuciosamente explicamos en el caso anterior, que:

á la suma de las funciones f, extensivas á todos los divisores de los términos comprendidos en el grupo ΣD_2, entre los cuales no figura el número N.

Y como se ha demostrado que en ambos grupos existen los mismos divisores, inferiores á N, resulta que ambas sumas,

$$\Sigma F(D_1) \quad \text{y} \quad \Sigma F(D_2),$$

sólo pueden diferir por la $f(N)$, que figura entre los sumandos de la primera, y no en la segunda. Luego, en conclusion:

$$f(N) = \Sigma F(D_1) - \Sigma F(D_2).$$

$$f(N) = \frac{\Pi F(D_1)}{\Pi F(D_2)} \quad (6$$

en la cual D_1 y D_2 conservan la significacion restringida que al definirlos se les asignó.

Si en la igualdad (5) suponemos que

$$F(N) = N = \Pi f(D),$$

la (6) se convertirá en esta otra:

$$f(N) = \frac{\Pi D_1}{\Pi D_2}.$$

Detengámonos un momento en la interpretacion de esta última igualdad.

Si $N = 1$, los números D_1 y D_2 serán iguales entre sí, é iguales á la unidad; y á la unidad equivaldrá tambien el cociente indicado en el segundo miembro.

Si N fuese un producto cualquiera de factores primos, fácil es comprender, recordando el procedimiento empleado en la demostracion de la propiedad de los números D_1 y D_2, que los productos ΠD_1 y ΠD_2 son tambien iguales entre sí; y por lo tanto, $f(N) = 1$.

Mas, si N fuese igual á un número primo, a, por ejemplo, sería

$$\Sigma D_1 - \Sigma D_2 = a - 1;$$

y, por consecuencia, los términos comprendidos en el grupo ΣD_1 quedarían reducidos al a, y en el segundo al 1. La funcion $f(N)$, que discutimos, sería entónces igual al número propuesto N ó a. Y lo propio sucedería si $N = a^\alpha$, ó igual á una potencia de un número primo; porque, en este supuesto, sería

$$\Sigma D_1 - \Sigma D_2 = a^{\alpha-1}(a-1) = a^\alpha - a^{\alpha-1};$$

y los términos D_1 se reducirian á a^α y los D_2 á $a^{\alpha-1}$; cuyo co-

ciente, ó la funcion $f(N)$, es igual al mismo número a, base del propuesto $N = a^{\alpha}$.

Para terminar este capítulo, y por el interés que ofrece, insertamos á continuacion una tabla de los valores de $\varphi(N)$ para los 100 primeros números.

VALORES DE φ.

1	1	21	12	41	40	61	60	81	54
2	1	22	10	42	12	62	30	82	40
3	2	23	22	43	42	63	36	83	82
4	2	24	8	44	20	64	32	84	24
5	4	25	20	45	24	65	48	85	64
6	2	26	12	46	22	66	20	86	42
7	6	27	18	47	46	67	66	87	56
8	4	28	12	48	16	68	32	88	40
9	6	29	28	49	42	69	44	89	88
10	4	30	8	50	20	70	24	90	24
11	10	31	30	51	32	71	70	91	72
12	4	32	16	52	24	72	24	92	44
13	12	33	20	53	52	73	72	93	60
14	6	34	16	54	18	74	36	94	46
15	8	35	24	55	40	75	40	95	72
16	8	36	12	56	24	76	36	96	32
17	16	37	36	57	36	77	60	97	96
18	6	38	18	58	28	78	24	98	42
19	18	39	24	59	58	79	78	99	60
20	8	40	16	60	16	80	32	100	40

CAPITULO IV.

De la congruencia de los números.

59.—*Definiciones.*

Elegido, como tipo (38), cualquier número entero, k, todos los demás enteros pueden ser representados, mediante aquél, por la forma

$$sk + r.$$

en la cual s representa tambien un entero, y r uno de los k números

$$0,\ 1,\ 2,\ \ldots\ (k-1).$$

Entre cada dos múltiplos consecutivos de k existirán siempre k números, á saber:

$$sk,\ sk+1,\ sk+2\ldots\ sk+(k-1);$$

de modo que en la forma general,

$$a = sk + r,$$

á cada valor de s corresponden k valores de r; y, si hacemos que s recorra sucesivamente todos los enteros, desde $-\infty$ hasta $+\infty$, la forma mencionada representará todos los números a. Mas no basta decir ésto para determinar completamente la forma en cuestion, sino que es necesario añadir que, por el procedimiento explicado, la forma $sk+r$ produce una vez sola cada uno de los números a. Para demostrar este aserto supongamos, por un momento, que sean iguales dos valores de esta forma, á saber:

$$s'k + r' = sk + r.$$

De esta igualdad se deduce esta otra

$$(r' - r) = (s - s')\,k\,;$$

ahora bien, r' es uno de los k números,

$$0\,.\ 1\,.\ 2\,.\,.\,.\,.\ (k-1\ .$$

y el valor absoluto de la diferencia $(r' - r)$ es al mismo tiempo uno de estos números; pero, segun la última igualdad, $(r' - r)$ debe ser múltiplo de k: luego necesariamente

$$r' - r = 0$$

y, por consecuencia,

$$r' = r\,,\quad \text{y}\quad s' = s.$$

En adelante llamarémos al número r *resto* del número a, respecto del tipo k, que se denomina *módulo*. Dos ó más números que produzcan iguales *restos*, respecto de un mismo *módulo*, se llaman *cóngruos* ó *congruentes* (Gauss), ó *equivalentes* (Cauchy).

La congruencia entre dos números a, b, la escribe *Gauss* con un signo especial, semejante al de igualdad, de este modo:

$$a \equiv b\,(\text{mod. } k)\,;$$

y los franceses, en general, valiéndose efectivamente del signo de igualdad, de este otro:

$$a = sk + b.$$

Siendo a y b *congruentes*, respecto del *módulo* k, y r su *resto* comun, tendremos, segun la definicion y modos de escribir las congruencias,

$$a \equiv r\,(\text{mod. } k)\,,$$

$$b \equiv r\,(\text{mod. } k)\,,$$

ó bien, las igualdades

$$a = sk + r$$

$$b = s'k + r\,:$$

de donde se deduce esta otra:

$$(a - b) = (s - s')\,k$$

la cual, en lenguaje vulgar, expresa que *la diferencia entre dos números congruentes es divisible por el módulo;* y tambien que la recíproca es cierta; puesto que, si a y b diesen restos distintos, tendrian las formas

$$a = sk + r$$
$$b = s'k + r';$$

y de ellas resulta la igualdad

$$(a - b) = (s - s')\,k + (r - r');$$

de la cual se desprende que, si por hipótesis fuese $(a - b)$ divisible por k, tendria tambien que serlo (39-4.ª) la diferencia de los restos $(r - r')$: lo cual, segun hemos dicho ha poco, exige que éstos sean iguales, esto es, $r = r'$, ó bien que los números a, b sean *congruentes.*

Podemos, en consecuencia, decir tambien que son *congruentes* dos números cuya diferencia es divisible por el *módulo;* y además que cada uno de dos números congruentes es *resto* del otro.

60.—*Restos y no-restos de un módulo.*

Conforme con estas definiciones, todo número a es *congruente* con el *resto* r que resulta de dividirlo por el *módulo* k; en signos:

$$a \equiv r \,(\text{mod. } k).$$

Sin dejar de ser exacta esta congruencia, y permaneciendo a constante, puede recorrer el resto r, tomado en su más general acepcion, las dos séries de valores,

$$a,\ a - k,\ a - 2k,\ a - 3k, \ldots\ldots$$
$$a + k,\ a + 2k,\ a + 3k, \ldots\ldots$$

Así, por ejemplo, la congruencia

$$22 \equiv r \,(\text{mod. } 5)$$

no se altera, aunque se sustituyan por r los valores de la série

$$22,\quad 17,\quad 12,\quad 7,\quad 2,\quad -3,\quad -8.....$$

En general, si se verifica la congruencia,

$$a \equiv r \,(\text{mod. } k),$$

se verificará tambien esta otra:

$$a \equiv (r \pm mk) \,(\text{mod. } k);$$

en la cual es $r \pm mk$, suponiendo que m recorra los números 0, 1, 2....., la forma general de los restos del número a, respecto del módulo k. Todos los números, por el contrario, no comprendidos en tal forma, serán *incongruentes* con a, ó *no-restos* de a, respecto del módulo k.

Entre estos restos, salvo contadas excepciones, sólo se consideran los menores que el módulo, llamados *mínimos*, ya positivos, ya negativos, cuyas formas respectivas son:

$$\begin{aligned} &(a - mk) && \text{para los positivos,} \\ -&\{(m+1)k - a\} && \text{para los negativos,} \end{aligned}$$

cuando el número a se halle comprendido entre los múltiplos consecutivos del módulo, mk y $(m+1)k$. Concretándonos, pues, á estos restos *mínimos*, resulta que un número cualquiera tendrá dos, cada uno de los cuales figurará en una de las séries siguientes:

$$\begin{aligned} &0,\quad 1,\quad 2,..... \quad (k-1) \\ &0,-1,-2,..... \quad -(k-1), \end{aligned}$$

siendo, por consecuencia, uno positivo y otro negativo, escepto en el caso de que el resto del número dado sea cero.

Las formas de los restos, anteriormente escritas, prueban que la suma de los dos restos correspondientes á un módulo, fuera del signo, es igual á este módulo; pero, siempre que los valores absolutos de tales restos sean diferentes, uno de ellos será menor que la mitad del módulo; y los dos iguales á esta mitad, en el caso contrario. Estos restos menores ó, cuando más, iguales á la mitad del módulo, se llaman *mínimos absolutos*, y á ellos nos referiremos con frecuencia en nuestras ulteriores investigaciones. Estos restos *mínimos absolutos*, cuando el módulo k es par, están comprendidos en la série

$$1,\ 2,\ 3,\ldots\ldots +\frac{k-2}{2},\ \pm\frac{k}{2},\ -\frac{k-2}{2},\ldots\ldots -3,\ -2,\ -1;$$

y, cuando k sea impar, en esta otra:

$$1,\ 2,\ 3,\ldots\ldots +\frac{k-1}{2},\qquad -\frac{k-1}{2},\ldots\ldots -3,\ -2,\ -1.$$

Ejemplo. El resto mínimo, positivo, de 13 (mod. 5) es 2, tambien mínimo absoluto, y el negativo -3; respecto del módulo 7, el número 5 es él mismo su resto mínimo, positivo; y el negativo es -2, que es al mismo tiempo mínimo absoluto.

61.—*Propiedades de los números congruentes.*

1.° *Designando a y k dos enteros cualesquiera, se verificará siempre la congruencia*

$$a \equiv a \,(\text{mod. } k);$$

lo cual es evidente.

2.° *Si tienen lugar las congruencias*

$$a \equiv b \,(\text{mod. } k)$$

$$b \equiv c \,(\text{mod. } k)$$

se verificará tambien esta otra:

$$a \equiv c \,(\text{mod. } k).$$

Puesto que los restos de los tres números a, b, c, respecto del módulo k, son iguales entre sí.

3.ª *De las congruencias,*

$$a \equiv b \,(\text{mod. } k)$$

$$m \equiv n \,(\text{mod. } k),$$

se desprende esta otra:

$$(a \pm m) \equiv (b \pm n) \,(\text{mod. } k).$$

En efecto, segun la hipótesis, las diferencias, $(a - b)$ y $(m - n)$, son múltiplos del módulo k; luego tambien lo serán su suma y su diferencia (39–4.ª), á saber:

$$(a - b) \pm (m - n) = (a \pm m) - (b \pm n) = \textit{múltiplo} \text{ de } k,$$

cuya última igualdad demuestra el teorema.

Generalizando esta ley se puede enunciar diciendo:

Dada una série de congruencias, respecto al mismo módulo, se pueden sumar y restar ordenadamente, y los resultados de estas operaciones serán tambien congruentes, segun el módulo comun.

4.ª *Si se verifican las congruencias,*

$$a \equiv b \,(\text{mod. } k)$$

$$m \equiv n \,(\text{mod. } k),$$

será tambien cierta la congruencia,

$$am \equiv bn \,(\text{mod. } k).$$

Pues, siendo $(a - b)$, segun la hipótesis, múltiplo de k, lo será tambien

$$(a - b)\,m = am - bm,$$

ó, en otros signos, será

$$am \equiv bm \,(\text{mod. } k);$$

y, siendo tambien $(m - n)$ múltiplo de k, y, por consecuencia,

$$(m - n)\,b = bm - bn;$$

ó, en otros términos,

$$bm \equiv bn \,(\text{mod. } k),$$

será (2.ª) en conclusion

$$am \equiv bn \,(\text{mod. } k):$$

que es lo que pretendíamos demostrar.

Esta ley puede, como la anterior, generalizarse diciendo:

Dada una série de congruencias, respecto al mismo módulo, pueden multiplicarse ordenadamente, y los productos respectivos serán tambien congruentes.

Corolario. Si los números congruentes que figuran en los primeros miembros de las congruencias fuesen iguales entre sí, y los de los segundos miembros tambien, al multiplicarlas ordenadamente, obtendríamos potencias en vez de productos, y la ley anterior se convertiria en esta otra:

Las potencias del mismo grado de dos números congruentes son asimismo congruentes.

5.ª De la igualdad

$$\frac{a - b}{k} = \frac{am - bm}{km},$$

cuyos dos miembros expresan respectivamente las congruencias

$$a \equiv b \,(\text{mod. } k),$$

y

$$am \equiv bm \,(\text{mod. } km),$$

se deduce la proposicion:

Si los dos miembros y el módulo de una congruencia contienen un factor comun, puede este suprimirse sin que la congruencia se altere.

Así, por ejemplo, en la congruencia

$$12x \equiv -3 \,(\text{mod. } 15)$$

puede suprimirse el factor 3 contenido en sus dos miembros y el módulo, y se obtiene esta otra:

$$4x \equiv -1 \,(\text{mod. } 5).$$

6.ª *Dada la congruencia de dos números, a y b, segun diferentes módulos,*

$$k_1,\ k_2,\ k_3,\ \ldots\ldots \text{ etc.},$$

á saber:

$$a \equiv b \,(\text{mod. } k_1),\quad a \equiv b \,(\text{mod. } k_2),\quad a \equiv b \,(\text{mod. } k_3)\ldots\ldots,$$

se verificará tambien la que sigue:

$$a \equiv b \,(\text{mod. } \mu),$$

donde μ representa el mínimo comun múltiplo de los módulos

$$k_1,\ k_2,\ k_3\ldots\ldots$$

Puesto que, segun la hipótesis, la diferencia $a - b$ es divisible por todos los números

$$k_1,\ k_2,\ k_3\ldots\ldots;$$

y, por consecuencia, lo será por el *mínimo comun múltiplo* μ de estos divisores.

Si los módulos

$$k_1,\ k_2,\ k_3\ldots\ldots$$

fuesen primos entre sí dos á dos, los números, a y b, serían congruentes, segun el producto de todos aquellos, el cual forma, en este caso (44-Cor.), *su mínimo comun múltiplo.*

7.ª *Dada la congruencia*

$$a \equiv r \,(\text{mod. } k'\,k'')$$

y estas otras dos, correspondientes á cada uno de los factores del módulo de la primera,

$$a \equiv r' \ (\text{mod. } k')$$

$$a \equiv r'' \,(\text{mod. } k''),$$

se verificarán tambien entre los restos de las tres, las siguientes:

$$r \equiv r' \ (\text{mod. } k')$$

$$r \equiv r'' \,(\text{mod. } k'').$$

En efecto, escribiendo en forma de igualdad las congruencias referentes á la hipótesis, siendo m, n, p, números enteros, tendremos:

$$a = m k' k'' + r$$

$$a = n k' \quad + r'$$

$$a = p k'' \quad + r'' ;$$

de las cuales se deducen las que siguen:

$$r = (n - m k'')\, k' \ + r'$$

$$r = (p - m k')\, k'' + r''.$$

que demuestran la conclusion.

8.ª *Dada la congruencia*

$$a m \equiv b m \,(\text{mod. } k),$$

no puede, sin excepcion, asegurarse que se verificará tambien esta otra:

$$a \equiv b \,(\text{mod. } k).$$

En efecto, sea δ el máximo comun divisor del factor comun m, que figura en la primera congruencia, y de su módulo k; y designemos por

m' y k' los cocientes resultantes de dividir por δ respectivamente m y k. De la congruencia citada se desprende que $(a - b)m$ es divisible por k; y de aquí, que $(a - b)m'$ debe serlo tambien por k'; pero, como m' y k' son primos entre sí (42-T.), necesariamente (41-2.°) tendrá que ser $(a - b)$ divisible por k': luego de la congruencia

$$am \equiv bm \,(\text{mod. } k)$$

sólo puede, en general, deducirse esta otra:

$$a \equiv b \,(\text{mod. } k').$$

Mas, si el factor comun m y el módulo k, en la congruencia dada, fuesen primos relativos, sería $\delta = 1$; y entónces se verificaria siempre tambien la congruencia

$$a \equiv b \,(\text{mod. } k);$$

lo cual manifiesta: *que los dos miembros de una congruencia pueden ser divididos, sin que se altere, por un factor comun, primo con el módulo.*

Corolario. Una congruencia

$$am \equiv bn \,(\text{mod. } k)$$

será divisible por otra

$$m \equiv n \,(\text{mod. } k)$$

siempre que los dos miembros de la segunda sean primos con el módulo comun de ambas.

En efecto, de esta última se deduce (4.ª) la siguiente:

$$am \equiv an \,(\text{mod. } k),$$

que, en combinacion con la primera, nos da esta otra:

$$an \equiv bn \,(\text{mod. } k);$$

ó bien, como n es primo con k por hipótesis,

$$a \equiv b \,(\text{mod. } k):$$

congruencia que representa el cociente de dividir ordenadamente las dos propuestas.

8. Las propiedades referentes á la adicion, sustraccion, multiplicacion y elevacion á potencias de los números congruentes, pueden compendiarse de este modo:

Si $f(x, y, z.....)$ *representa una funcion racional, entera y con coeficientes enteros, de las indeterminadas* $x, y, z.....$, *y se verifican las congruencias,*

$$a \equiv a', \quad b \equiv b', \quad c \equiv c'..... \text{ (mod. } k),$$

será tambien cierta esta otra:

$$f(a, b, c.....) \equiv f(a', b', c'.....) \text{ (mod. } k).$$

Nota. Aunque sólo hemos hablado anteriormente de módulos positivos, adviértase, sin embargo, que la misma significacion tienen los números congruentes para los módulos negativos.

62.—*Sistema completo de números incongruentes.*

De los principios demostrados (59) se deduce que todo número a es congruente con su resto respecto de un módulo cualquiera k, y, por consecuencia, congruente con uno, y uno solo, de los términos de la série de los restos de k,

$$0, \quad 1, \quad 2, ... \quad (k-1).$$

Tomando, pues, por tipo de comparacion, ó módulo, un número arbitrario k, es evidente que todos los números enteros podremos distribuirlos en k clases, figurando en cada una de ellas exclusivamente los números congruentes (mod. k) con cada uno de los k restos mínimos positivos que constituyen la série poco antes expresada. Es decir, en una clase deberán estar comprendidos todos los números divisibles por k ó, en otros términos, $\equiv 0$ (mod. k); pero nada más que ellos so-

los; en otra los números $\equiv 1 \pmod{k}$; en una tercera los $\equiv 2 \pmod{k}$; y así sucesivamente.

Si de cada una de estas k clases diferentes elegimos un individuo cualquiera, formaremos un sistema compuesto de k números que posee la notable propiedad de que alguno, y uno solo, de sus términos es congruente con cualquier número entero, comparados ambos con el mismo módulo k. Este sistema, como lo es en efecto el de los números

$$0, \quad 1, \quad 2, \ldots\ldots (k-1),$$

lleva el nombre de *sistema completo de restos*, ó *sistema completo de números incongruentes*, respecto del módulo k.

Es claro, segun lo dicho, que los números

$$1, \quad 2, \quad 3, \ldots\ldots k$$

constituyen tambien un *sistema completo de números incongruentes;* y que forma, en general, un sistema de esta especie cualquiera série de k números enteros, consecutivos.

Todos los individuos comprendidos en cada una de las clases enumeradas poseen várias cualidades comunes, y representan, con relacion al módulo, el papel de un individuo solo. Ya hemos visto, para corroborar este aserto, que una congruencia no se altera aunque sustituyamos cualquier sumando ó factor que figuren en ella por otros números congruentes con los mismos.

Tambien se deduce de la equivalencia entre dos números, a y b,

$$a = b + sk,$$

que todo divisor comun al módulo k, y á uno de ellos a, lo es tambien del otro b, y del mismo módulo; es decir, que los números congruentes poseen un máximo divisor, comun con el módulo.

Tomando, pues, por base este elemento, ó divisor comun, podemos dividir los números tambien en clases de modo que cada una de ellas contenga todos los números cuyo máximo comun divisor sea uno de los divisores del módulo. Ahora bien, como segun acabamos de manifestar, todas las clases de números incongruentes, segun el módulo k, están

representadas por el sistema completo de restos

$$1,\ 2,\ 3.....\ k;$$

si designamos por δ un divisor cualquiera de k, y establecemos la igualdad consiguiente $k = n\delta$, será (56) $\varphi(n)$ el número de las clases que contienen números cuyo máximo divisor, comun con k, es δ (*). Y, como caso particular, representará tambien $\varphi(k)$ el número de las clases cuyos individuos sean todos primos con el módulo k.

63.—*Proposiciones fundamentales.*

Definido lo que se entiende por un sistema completo de restos, ó de números incongruentes, vamos á demostrar ahora, con la minuciosidad que su importancia merece, las proposiciones que siguen:

1.ª *Si los números a y k son primos entre sí, los restos resultantes de dividir por k, los $(k-1)$ múltiplos sucesivos de a,*

$$a\quad 2a\quad 3a.....\ (k-1)a,$$

son todos diferentes.

En efecto, si admitiésemos que dos cualesquiera de estos múltiplos, ma y na, por ejemplo, verificáran la congruencia

(*) Los números divisibles por δ en la série

$$1.\ 2.\ 3.....\ k.$$

son evidentemente

$$\delta,\ 2\delta,\ 3\delta,.....\ \frac{k}{\delta}\delta = n\delta.$$

Ahora bien, para que δ sea, en efecto, el máximo comun divisor de uno de estos últimos números, $s\delta$, por ejemplo, y de k, es necesario que los cocientes s y n que resultan de dividir por δ los números $s\delta$ y k, sean primos entre sí; pero $\varphi(n)$ expresa cuántos números primos con n existen en la série

$$1.\ 2.\ 3.....\ n;$$

luego tambien expresará cuántos tienen con k el máximo comun divisor δ en la série

$$1.\ 2.\ 3.....\ k.$$

$$ma \equiv na \,(\text{mod. } k),$$

tendria tambien que verificarse necesariamente esta otra:

$$m \equiv n \,(\text{mod. } k);$$

puesto que a es primo con k (7.ª). Pero m y n son, los dos, menores que k, y no podrán ser congruentes, ó lo que es lo mismo, no podrá ser divisible por k su diferencia, sino en el único caso de ser ésta cero, y, por consecuencia, m y n iguales; lo cual es contrario á la hipótesis: luego los expresados múltiplos de a son todos incongruentes (mod. k).

De otro modo podremos decir:

Si a y k son primos relativos, los términos de la serie

$$a, \quad 2a, \quad 3a, \ldots\ldots \quad (k-1)a$$

son, prescindiendo del órden, congruentes (mod. k) *con los de la série de restos*

$$1, \quad 2, \quad 3 \ldots\ldots \quad k-1.$$

O bien:

Si en la expresion ax, siendo a primo con k, damos á x sucesivamente los valores de un sistema completo de números incongruentes respecto de k, los valores correspondientes de los productos ax formarán tambien un sistema completo de números incongruentes (mod. k).

2.ª *Siendo a y k primos, en la série interminable,*

$$b, \quad b+a, \quad b+2a, \quad b+3a \ldots\ldots$$

los términos que ocupan los lugares

$$k, \quad 2k, \quad 3k \ldots\ldots \; etc.,$$

dan restos iguales; y cada grupo de k términos consecutivos produce restos diferentes, segun el módulo k.

En efecto, designemos por

$$b+ma \quad \text{y} \quad b+na$$

respectivamente los términos que en la série propuesta ocupan los luga-

res k y $2k$; en cuyo caso será evidentemente

$$n = m + k:$$

y escribamos las congruencias

$$\left.\begin{aligned} b + ma &\equiv r \\ b + na &\equiv r' \end{aligned}\right\} \text{(mod. } k\text{)}.$$

De estas dos congruencias se deduce (3.ª) esta otra:

$$(n - m)\,a \equiv (r' - r) \text{ (mod. } k\text{)}:$$

ó bien, sustituyendo por n su valor $m + k$, la siguiente:

$$ka \equiv (r' - r) \text{ (mod. } k\text{)}.$$

Pero ka es. como se ve, múltiplo de k, es decir:

$$ka \equiv 0 \text{ (mod. } k\text{)}:$$

luego, comparando las dos últimas congruencias, resulta que $r' - r$ tiene que ser *cero;* y, por tanto, iguales r y r': con lo cual está demostrada la primera parte de nuestro teorema.

Para demostrar la segunda basta considerar que siendo a y k primos entre sí, para que un múltiplo cualquiera, ax, de a, sea divisible por k, es necesario (41-2.°) que x sea divisible por k; y, si esta condicion no se cumple, segun la demostracion anterior, no producirán restos iguales los múltiplos ax.

De otro modo podemos tambien aquí decir:

Los términos de la série

$$b, \quad b + a, \quad b + 2a, \quad b + 3a \ldots\ldots \quad b + (k - 1)a$$

son congruentes (mod. k), *cualquiera que sea* b, *con los de la série natural*

$$1, \quad 2, \quad 3 \ldots\ldots \quad k - 1.$$

O bien que

La expresion $ax + b$, *siendo* a *primo con* k, *puede hacerse congruente, segun el módulo* k, *con cualquier número dado.*

3.ª Las dos proposiciones que anteceden se compendian en la siguiente: (*)

Si a *es primo con* k, *y en la expresion* $ax+b$ *sustituimos por* x *un sistema completo de números incongruentes* (mod. k), *los valores correspondientes de dicha expresion formarán tambien un sistema completo de números incongruentes* (mod. k).

En efecto, si admitimos que dos valores cualesquiera de la expresion mencionada son congruentes (mod. k); ó, hablando de otro modo, si suponemos que se verifica la congruencia

$$av+b \equiv at+b \,(\text{mod. } k),$$

tendrá por necesidad que verificarse la siguiente:

$$av \equiv at \,(\text{mod. } k);$$

y, por consecuencia, siendo a primo con k (61-8.ª), esta otra:

$$v \equiv t \,(\text{mod. } k).$$

La cual manifiesta que la congruencia entre dos valores,

$$av+b \quad \text{y} \quad at+b,$$

de la expresion propuesta $ax+b$, exige que sean tambien congruentes los dos valores v, t, de la indeterminada x que figura en ella: luego, si damos á esta indeterminada x, todos los k valores de un sistema completo de restos (mod. k), los valores correspondientes de la expresion $ax+b$ serán incongruentes; y, como no pueden distribuirse sino en k clases, formarán asimismo un *sistema completo* de tales números, segun el módulo k.

64.—*Teorema de Euler.*

Enunciadas y demostradas, hasta con prolijidad, las últimas proposiciones, la demostracion de este importantísimo teorema no presenta ya dificultad alguna.

(*) Gauss, *Disquisitiones arithmeticæ*, §§. 24 y 26.

Sustituyamos, pues, sucesivamente por x, en el producto ax, donde se supone a primo con k, un sistema de números á la vez primos é incongruentes con el módulo k, los cuales designamos por

$$a_1,\ a_2,\ a_3\ldots\ldots,$$

y cuyo número sabemos (56) es $\varphi(k)$. Los productos resultantes de tal sustitucion, á saber:

$$aa_1,\ aa_2,\ aa_3\ldots\ldots$$

poseerán tambien la doble propiedad de ser incongruentes y primos con k, y, por consecuencia, los restos respectivos

$$r_1,\ r_2,\ r_3\ldots\ldots$$

de dichos productos, segun k, coincidirán, aunque en orden diferente, con los números

$$a_1,\ a_2,\ a_3\ldots\ldots;$$

siendo, por tanto, el producto de estos números, $a_1\,a_2\,a_3\ldots\ldots$, igual al producto $r_1\ r_2\ r_3\ldots\ldots$ de los mencionados restos. Escribiendo, pues, las congruencias

$$\left.\begin{aligned} aa_1 &\equiv r_1 \\ aa_2 &\equiv r_2 \\ aa_3 &\equiv r_3 \\ &\vdots\quad\vdots \end{aligned}\right\} \pmod{k}$$

y multiplicándolas ordenadamente, obtendremos esta otra:

$$a^{\varphi(k)}\,a_1\,a_2\,a_3\ldots\ldots \equiv r_1\ r_2\ r_3\ldots\ldots \pmod{k};$$

de la cual, como los productos iguales

$$a_1\,a_2\,a_3\ldots\ldots \text{ y } r_1\ r_2\ r_3\ldots\ldots$$

son primos con k, se deduce (61–8.ª) la siguiente:

$$a^{\varphi(k)} \equiv 1 \pmod{k}$$

que expresa el teorema de Euler (*).

(*) *Euleri Commentationes arithmeticæ*, XX—55.

Traducida esta congruencia al lenguaje vulgar, dice así:

Siempre que a *represente un número primo con* k, *la potencia* $a^{\varphi(k)}$ *del primero, cuyo exponente designa cuántos números, primos é inferiores á* k, *existen en la série natural*

$$1.\ 2.\ 3.\ \ldots\ k.$$

es congruente con la unidad respecto del segundo; ó bien, la potencia $a^{\varphi(k)}$ *de* a *disminuida en la unidad, es divisible por* k.

Ejemplo. Sean

$$k = 24 \quad \text{y} \quad a = 31.$$

Los números primos é inferiores á 24 son

$$1.\ 5.\ 7,\ 11,\ 13,\ 17.\ 19,\ 23:$$

ó, en suma:

$$\varphi(24) = 8.$$

Multiplicando por cada uno de estos números sucesivamente el número dado $a = 31$, y fijándonos en los restos mínimos absolutos (60) de estos productos, respecto de $k = 24$, resultan las congruencias siguientes:

$$\left.\begin{array}{l} 1.31 \equiv 7 \\ 5.31 \equiv 11 \\ 7.31 \equiv 1 \\ 11.31 \equiv 5 \\ 13.31 \equiv 19 \\ 17.31 \equiv 23 \\ 19.31 \equiv 13 \\ 23.31 \equiv 17 \end{array}\right\} \text{ó bien} \left\{\begin{array}{l} 1.31 \equiv 7 \\ 5.31 \equiv 11 \\ 7.31 \equiv 1 \\ 11.31 \equiv 5 \\ -11.31 \equiv -5 \\ -7.31 \equiv -1 \\ -5.31 \equiv -11 \\ -1.31 \equiv -7 \end{array}\right\} \pmod{24}$$

Multiplicándolas ordenadamente, y suprimiendo de ambos miembros los productos compuestos de factores iguales, se llega, por fin, á esta otra:

$$31^8 \equiv 1 \text{ (mod. } 24)\text{;}$$

que puede comprobarse directamente, si se quiere, elevando 31 á la potencia 8 y dividiendo luego por 24.

Adviértase que algunas potencias de a, cuyo exponente sea inferior á $\varphi(k)$, pueden producir tambien el resto 1 respecto del módulo k. Así acontece, efectivamente, en el ejemplo anterior, donde la potencia segunda, y la cuarta, de 31, dan el mismo resto 1, respecto del módulo 24: es decir que, además de la congruencia de *Euler*

$$31^8 \equiv 1 \text{ (mod. } 24)\text{,}$$

se verifican tambien estas otras dos:

$$\left.\begin{array}{l} 31^4 \equiv 1 \\ 31^2 \equiv 1 \end{array}\right\} \text{(mod. } 24)$$

Escólio. Si el módulo k afectase la forma

$$k = p^{\pi}\, r^{\rho}\, s^{\sigma} \ldots\ldots$$

será, como sabemos (55),

$$\varphi(k) = (p-1)p^{\pi-1}.(r-1)\,r^{\rho-1}.(s-1)\,s^{\sigma-1} \ldots\ldots\text{;}$$

y la congruencia de Euler, por consecuencia, se podrá escribir de este modo:

$$a^{(p-1)p^{\pi-1}(r-1)r^{\rho-1}(s-1)s^{\sigma-1}} \equiv 1 \text{ (mod. } p^{\pi}\, r^{\rho}\, s^{\sigma} \ldots\ldots)$$

en cuya expresion representan p, r, s..... números primos absolutos, diferentes, y a otro número cualquiera, no divisible por ninguno aquellos.

65.—*Teorema de Fermat.*

Este teorema es realmente un caso particular del de Euler, que se llama por esta razon tambien *Teorema de Fermat generalizado.*

En efecto, supongamos primeramente que sea $k = p^{\pi}$ la potencia π de un número primo p. En este caso será (55–Esc.)

$$\varphi(k) \quad \varphi(p^{\pi}) - p \quad 1\ p^{\pi-1};$$

y la congruencia de Euler, anteriormente demostrada, se convertirá, por consecuencia, en la siguiente:

$$a^{p-1)p^{\pi-1}} \equiv 1 \pmod{p^{\pi}};$$

donde a representa un número cualquiera, no divisible por el número primo p.

Si suponemos ahora que el exponente π de p en la última congruencia sea igual á la unidad, resultará esta otra

$$a^{p-1} \equiv 1 \pmod{p}.$$

que expresa el teorema de *Fermat.*

Este teorema en lenguaje vulgar dice así:

Si p es un número primo, y a otro número cualquiera, no divisible por el primero, la potencia a^{p-1} del segundo, cuyo exponente es dicho número primo ménos la unidad, dividida por este mismo número primo, produce el resto 1.

Multiplicando por a los dos miembros de la congruencia de *Fermat*, tendremos la que sigue:

$$a^{p} \equiv a \pmod{p};$$

que se verifica siempre que a sea divisible por p, en atencion á que entónces sus dos miembros son $\equiv 0 \pmod{p}$. Mas, si en esta congruencia suponemos que a no sea divisible por p, en cuyo caso es

primo con éste, pueden dividirse (61-8.ª) por a sus dos miembros, y así volver á la de *Fermat*

$$a^{p-1} \equiv 1 \pmod{p}.$$

66.—*Otra demostracion de los mismos teoremas.*

Entre las varias, además de las dichas, que por diferentes matemáticos se han publicado, ofrece particular interés para nosotros la que sigue (*):

Sabemos (33) que los coeficientes del desarrollo de la potencia de un binomio, formulado simbólicamente por la igualdad

$$(a+b)^n = \sum n^{.\alpha}\, a^{n-\alpha}\, b^{\alpha},$$

en la cual n es entero y positivo, son todos enteros; é iguales á la unidad los de los términos extremos a^n, b^n, de dicho desarrollo, que corresponden á los valores tambien extremos que puede recibir α, á saber:

$$\alpha = 0, \quad \alpha = n.$$

Los mencionados coeficientes, exceptuando naturalmente el primero y el último que acabamos de decir son iguales á la unidad, satisfacen además á la condicion de ser divisibles por n siempre que este exponente sea un número primo; puesto que la forma general (22) de los mismos,

$$n^{.\alpha} = \frac{n!}{\alpha!\,(n-\alpha)!}$$

que contiene evidentemente al n en su numerador y no le contiene en su denominador, puede escribirse de este otro modo:

$$n\,\frac{r}{s}$$

(*) *Gauss.*—D. A. §.—5]

y así claramente se deduce que, por ser n primo con s y entero el coeficiente $\frac{nr}{s}$, el cociente $\frac{r}{s}$ representa tambien un entero.

Siendo, pues, divisibles por n, ó en otros términos, $\equiv 0 \pmod{n}$, todos los términos del desarrollo antes indicado, ménos el primero y el último, sin inconveniente podemos establecer la congruencia

$$(a+b)^n \equiv a^n + b^n \pmod{n};$$

de la cual, por el procedimiento explicado en el número (34), para pasar del caso de un binomio al general de un polinomio, se deduce la que sigue, despues de cambiar la letra n por la p:

$$(a+b+c+\ldots\ldots)^p \equiv a^p + b^p + c^p + \ldots\ldots \pmod{p}.$$

Suponiendo ahora que todos los términos a, b, c..... del polinomio elevado á p son iguales á la unidad, y designando por a su número, tendremos por fin la congruencia

$$a^p \equiv a \pmod{p}, \qquad (A)$$

que se verifica siempre que a sea entero y positivo, y, evidentemente cuando a sea cero.

Para demostrar que tambien se verifica cuando a sea negativo, basta tener presente que la congruencia

$$(-1)^p \equiv -1 \pmod{p}$$

es cierta para todo número primo, impar; y que lo es tambien esta otra

$$(-1)^2 \equiv -1 \pmod{2}$$

para el único número primo, par, 2; es decir, que para *todos* los números primos se verifica la congruencia

$$(-1)^p \equiv -1 \pmod{p} \qquad (B)$$

Si se multiplican ordenadamente las congruencias (A) y (B), resulta (61-4.°) esta otra:

$$(-a)^p \equiv -a \text{ (mod. } p)\text{;}$$

de donde se concluye que la (*A*) es cierta para todo número entero, a. positivo, negativo ó cero.

La congruencia

$$a^p \equiv a \text{ (mod. } p)\text{,}$$

expresa que *todo número* a *es congruente con su potencia* p, *esto es, con* a^p, *segun el módulo* p, *siendo este módulo un número primo.*

Y, si admitimos ahora la condicion de que a no sea divisible por p. en cuyo supuesto (45) el número a será primo con p, de la congruencia última

$$a^p \equiv a \text{ (mod. } p)\text{,}$$

se deducirá (61–8.ª) la siguiente:

$$a^{p-1} \equiv 1 \text{ (mod. } p)$$

ó, si se quiere, la igualdad

$$a^{p-1} = 1 + hp,$$

donde h es entero, que representa el teorema de *Fermat.*

Para pasar de este teorema al de *Euler* elevemos la última igualdad á la potencia p, y tendremos:

$$a^{(p-1)p} = 1 + h'p^2,$$

donde h' es un número entero; ó bien la congruencia

$$a^{(p-1)p} \equiv 1 \text{ (mod. } p^2).$$

Elevando de nuevo esta congruencia á la potencia p, obtendremos la siguiente:

$$a^{(p-1)p^2} \equiv 1 \text{ (mod. } p^3)\text{;}$$

y procediendo con esta congruencia del mismo modo, y con las que vayan sucesivamente resultando, llegaremos sin duda á esta otra:

$$a^{(p-1)p^{\pi-1}} \equiv 1 \text{ (mod. } p^\pi).$$

Congruencias semejantes á la última obtendremos para cualesquiera números primos, r, s, t..... que no sean divisores de a, á saber:

$$a^{(r-1)r^{\rho-1}} \equiv 1 \pmod{r^{\rho}}$$

$$a^{(s-1)s^{\sigma-1}} \equiv 1 \pmod{s^{\sigma}}$$

$$a^{(t-1)t^{\tau-1}} \equiv 1 \pmod{t^{\tau}}$$

.....

Si designamos por h el producto de todos los exponentes que figuran en sus primeros miembros, la congruencia

$$a^{h} \equiv 1$$

se verificará evidentemente con respecto á cualquiera de los módulos

$$p^{\pi}, \quad r^{\rho}, \quad s^{\sigma} \ldots\ldots$$

á que las anteriores congruencias se refieren; y, como estos módulos son primos entre sí, asimismo se verificará que

$$a^{h} \equiv 1 \pmod{p^{\pi} r^{\rho} s^{\sigma} \ldots\ldots}.$$

Pero, segun hemos supuesto, es

$$h = (p-1)p^{\pi-1}.\ (r-1)r^{\rho-1}.\ (s-1)s^{\sigma-1} \ldots\ldots = \varphi(p^{\pi} r^{\rho} s^{\sigma} \ldots\ldots):$$

luego la última congruencia expresa efectivamente el teorema de *Euler*, cuya nueva demostracion buscábamos.

PARTE SEGUNDA.

RESOLUCION DE LAS CONGRUENCIAS.

CAPITULO I.

De las congruencias de primer grado.

67.—*Definiciones generales.*

Despues de haber estudiado, en particular, los caractéres y propiedades de los números, sus clasificaciones, y las formas propias de los comprendidos en cada clase, nos corresponde tomar ahora por objeto de nuestras investigaciones, en general, las formas numéricas, ligadas entre sí como doble expresion de la misma cantidad, ó como equivalentes, y compuestas de elementos conocidos é indeterminados, cuyas mútuas relaciones y caractéres debemos inquirir con la mira de patentizar que la dependencia entre aquellas formas, bien respecto de sus partes, ya en cuanto á su conjunto, se halla justamente establecida.

La representacion, pues, de las *congruencias* en la Teoría de los Números es muy semejante á la de las *ecuaciones* en el Algebra: por cuya razon no diferirán gran cosa en su sentido ciertos términos en ambos casos empleados. Así, llamamos aquí tambien *miembros*, primero ó segundo, de una congruencia, á las expresiones ó formas que figuran respectivamente á la izquierda ó la derecha del signo $\equiv$; *incógnitas* á sus elementos indeterminados ó desconocidos; *coeficientes* á los factores de

estas incógnitas; y *raices* á los valores determinados de las mismas que transforman en otra, idéntica, la congruencia propuesta.

La forma general de la congruencia con una sola incógnita es ésta:

$$a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n \equiv 0 \pmod{k}$$

que tambien se escribe abreviadamente como sigue:

$$f(x) \equiv 0 \pmod{k},$$

y en la cual designa el exponente n un número entero y positivo, y los coeficientes

$$a_0,\ a_1,\ a_2 \ldots\ a_n;$$

números enteros, determinados.

Todo valor entero de x, que haga divisible por el módulo k el primer miembro de esta congruencia, es *raiz* de la misma. Mas acerca de estas raices hay que hacer una observacion de importancia, y peculiar de la *Teoría de los Números:* supongamos que el valor hallado de x, ó raiz de la congruencia dada, sea a; todos los números congruentes con a, esto es, todos los individuos de la clase (62) á que este número a pertenece, respecto del módulo k, son asimismo raices de la expresada congruencia, y en número infinito; pero todas ellas representan una sola raiz: luego el problema ó dificultad de *resolver* una congruencia se reduce á buscar todas sus raices *incongruentes;* teniendo sólo en cuenta, además, en cada una de estas clases de raices, las menores que el módulo, ó bien las comprendidas entre sus dos restos mínimos absolutos, extremos, negativo y positivo.

Es evidente tambien que toda raiz de la congruencia arriba escrita lo será asimismo de esta otra,

$$b_0 x^n + b_1 x^{n-1} + b_2 x^{n-2} + \cdots + b_{n-1} x + b_n \equiv 0 \pmod{k},$$

siempre que se verifiquen las relativas á sus coeficientes

$$a_r \equiv b_r \pmod{k}:$$

es decir, que dos congruencias,

$$f(x) \equiv 0 \text{ (mod. } k)$$

$$F(x) \equiv 0 \text{ (mod. } k)$$

son entre sí congruentes,

$$f(x) \equiv F(x) \text{ (mod. } k),$$

y pueden realmente considerarse como una sola, cuando sus coeficientes de iguales potencias de la incógnita sean tambien congruentes. Para hacer esta comparacion entre los coeficientes de las dos congruencias mencionadas pueden, sin obstáculo, suponerse iguales á cero cuantos falten en cualquiera de ellas, y debieran corresponder á los de iguales potencias de la incógnita en la otra.

Infiérese de lo dicho, que no hay inconveniente en suprimir de una congruencia todos los coeficientes divisibles por el módulo; y, efectuada esta supresion, el exponente de la mayor potencia restante de la incógnita se denomina *grado* de la congruencia. Así, por ejemplo, si el término permanente de la dada fuese el primero $a_0 x^n$ (y esto probaría que su coeficiente a_0 no era múltiplo del módulo k), dicha congruencia se llamaria de grado n.

Una congruencia se apellida *idéntica* cuando todos sus coeficientes son divisibles por el módulo: lo cual equivale á decir, que entónces no existe realmente semejante congruencia. Y una congruencia será imposible evidentemente, siempre que sus coeficientes sean divisibles por algunos de los factores del módulo, y no lo sea por los mismos su término independiente de x.

Es claro que todos los coeficientes de una congruencia pueden reducirse á sus restos mínimos, ó mínimos absolutos, respecto del módulo. Y, por último, que, segun se acostumbra en las ecuaciones, tambien puede, como veremos, reducirse á la unidad el coeficiente de la más elevada potencia de la incógnita, multiplicando todos los términos de la congruencia por un número cuyo producto por dicho coeficiente sea cóngruo con la unidad.

68.—*Congruencias de primer grado.*

Toda congruencia de primer grado ó *lineal,* despues de efectuada la *trasposicion* de sus términos, se reduce á la forma siguiente:

$$ax \equiv b \text{ (mod. } k\text{)}. \qquad (1)$$

En la resolucion de esta congruencia distinguiremos dos casos:

1.° *Cuando el coeficiente a de la incógnita sea primo con el módulo k.*

En este caso, segun la proposicion demostrada (63), es posible siempre encontrar un valor v de x, que haga el producto av congruente con el número b respecto de dicho módulo k; y, como cualquiera otro valor de x, por el cual se obtenga el mismo resultado que con el primero v, tiene que ser por precision congruente con éste, conforme enseña tambien el teorema aludido, conclúyese que la congruencia

$$x \equiv v \text{ (mod. } k\text{)}.$$

ó bien, la expresion

$$x = v + kz$$

representan la *solucion completa* de la congruencia dada.

Aplicando las denominaciones que al comenzar este capítulo recordamos, diremos que las raices de la congruencia de primer grado (1) son todas entre sí congruentes, ó pertenecen á la misma clase (62) respecto del módulo; y por consecuencia, aunque en número infinito, no deben considerarse sino como una *sola* raiz cuya forma general es

$$x = v + kz,$$

siendo z un número entero.

Esto sentado, para hallar efectivamente este valor v de x, ó resolver la congruencia propuesta,

$$ax \equiv b \text{ (mod. } k\text{)},$$

por medios ya conocidos, la compararemos con la de Euler (64)

$$a^{\varphi(k)} \equiv 1 \text{ (mod. } k)$$

y obtendremos en seguida

$$x \equiv b \,.\, a^{\varphi(k)-1} \text{ (mod. } k).$$

Ejemplo. Sea la congruencia cuya solucion buscamos

$$2x \equiv -3 \text{ (mod. } 15).$$

Como (55)

$$\varphi(15) = 8 \quad \text{y} \quad 2^7 = 128 \equiv -7 \text{ (mod. } 15),$$

tendremos:

$$x \equiv -3 \,.\, -7 \equiv 21 \equiv 6 \text{ (mod. } 15).$$

Luego la forma que comprende todas las *raizes* ó *soluciones* de la congruencia dada, y representa su única *clase*, es la siguiente:

$$x = 6 + 15z.$$

2.° *Cuando el coeficiente* a *de la incógnita no sea primo con el módulo* k.

Designando en este caso por δ el máximo comun divisor de los números a y k, desde luego se concibe que cualquier valor de x que satisfaga á la congruencia (1)

$$ax \equiv b \text{ (mod. } k),$$

satisfará tambien á la misma congruencia, segun el módulo δ; pero siempre será

$$ax \equiv 0 \text{ (mod. } \delta).$$

puesto que a es divisible por δ; por cuya razon, á no ser b tambien divisible por δ, esto es,

$$b \equiv 0 \text{ (mod. } \delta),$$

la congruencia (1) es irresoluble.

Admitida esta condicion *necesaria*, y, haciendo

$$a = a'\delta\,, \quad b = b'\delta\,, \quad k = k'\delta\,.$$

obtendremos la congruencia

$$a'x \equiv b' \,(\text{mod. } k')\,, \tag{2}$$

equivalente á la primera; porque no hay duda que será la diferencia $a'x - b'$ divisible por k', siempre que la otra, $a'\delta x - b'\delta$, lo sea por $k'\delta$; y recíprocamente. Siendo, pues, unas mismas las raices de las dos congruencias

$$ax \equiv b \,(\text{mod. } k) \quad \text{y} \quad a'x \equiv b' \,(\text{mod. } k')\,,$$

como el coeficiente a' de la incógnita en la última es (42-Cor.) primo con el módulo k', retrocedemos al caso anterior, siempre posible, y que ya sabemos resolver; de lo cual se desprende que la condicion calificada antes de *necesaria* para que fuese resoluble la congruencia (1), es además *suficiente*.

Ahora bien, segun hemos dicho en el primer caso, la congruencia

$$a'x \equiv b' \,(\text{mod. } k')$$

tendrá una infinidad de raices congruentes (mod. k'), cuya forma general, siendo v una de ellas, será

$$x = v + k'z\,. \tag{3}$$

Mas todas estas raices lo son tambien de la congruencia

$$ax \equiv b \,(\text{mod. } k)\,:$$

y es natural que ocurra preguntar cuántos de los números comprendidos en la expresion (3) serán incongruentes respecto del módulo k de esta última congruencia. Para averiguarlo, recordaremos (59) que dos números distintos,

$$v + zk' \quad \text{y} \quad v + z'k'\,,$$

de los mencionados (3), serán congruentes (mod. k) siempre que su diferencia.

$$(z - z')\,k'.$$

sea divisible por dicho módulo k; y para que ésto se verifique, como es $k = k'\delta$, es indispensable que $z - z'$ sea divisible por δ, ó, en otros términos, que se verifique la congruencia

$$z \equiv z' \,(\text{mod. } \delta).$$

Infiérese de aquí, que dos números cualesquiera de los comprendidos en la forma (3)

$$x = r + zk'.$$

pertenecerán á la misma clase, ó á clases diferentes, respecto del módulo k, segun que los números z y z' pertenezcan á la misma clase, ó á clases diferentes, respecto del módulo δ; concluyéndose que la multitud indefinida de los términos de la série abreviada

$$r + zk'.$$

puede distribuirse en δ clases diferentes, respecto del módulo k de la congruencia (1) propuesta. Y, en efecto: son los representantes de cada una de estas δ clases las δ formas numéricas que á continuacion se expresan:

$$r, \quad r + k', \quad r + 2k', \quad r + 3k', \ldots\ldots \quad r + (\delta - 1)\,k'.$$

El resultado, en lenguaje vulgar, de cuanto queda dicho, es el siguiente:

Para que una congruencia sin limitacion alguna

$$ax \equiv b \,(\text{mod. } k),$$

sea resoluble, ó contenga raices, es necesario que su segundo miembro b sea divisible por el máximo comun divisor δ del coeficiente a de la incógnita y del módulo k; y, si esta condicion se cumple, la congruencia propuesta contiene exactamente δ clases de raices, ó δ raices incongruentes, respecto de su módulo.

Es claro que la condicion aquí exigida se cumple siempre que sea $\delta = 1$, como sucede en el caso primero ya explicado; y cuando sea

$\delta = k$, en cuyo supuesto es

$$a \equiv 0 \pmod{k},$$

con tal que al mismo tiempo sea

$$b \equiv 0 \pmod{k},$$

se verifica tambien la condicion exigida en el resumen anterior; pues entónces cualquier número x satisface á la congruencia idéntica

$$ax \equiv b \pmod{k},$$

segun al principio de este párrafo afirmamos.

Por via de ejemplo del caso general nos propondremos resolver la congruencia

$$8x \equiv -12 \pmod{60}.$$

Ante todo observaremos que esta congruencia es posible; porque el máximo comun divisor, 4, del coeficiente 8, y el módulo 60, es divisor tambien de su segundo miembro — 12; y de aquí se deduce inmediatamente que tiene 4 raices.

Para encontrarlas dividamos la congruencia dada por 4 y obtendremos la siguiente:

$$2x \equiv -3 \pmod{15}$$

cuya única clase de raices está expresada, como sabemos (*caso* 1.°), por la forma

$$6 + 15z;$$

de la cual, haciendo

$$z = 0,\ 1,\ 2,\ 3,$$

resultan las cuatro clases de raices de la congruencia dada, á saber:

$$x \equiv 6,\quad x \equiv 21,\quad x \equiv 36,\quad x \equiv 51 \pmod{60}.$$

Tambien pudiéramos haber hecho depender la resolucion de la congruencia propuesta de dos congruencias, segun los módulos 4 y 15 respectivamente, mas viniendo siempre á parar en el primer caso de que antes tratamos.

Es evidente que el procedimiento explicado para hallar el valor de la incógnita, en los dos casos precedentes, se facilitaría mediante una tabla, semejante á la que figura en la página 134, que contuviera los $(k-1)$ múltiplos del coeficiente a de la incógnita y sus restos mínimos absolutos correspondientes, respecto del módulo k; mucho más teniendo en cuenta que cada dos múltiplos equidistantes de los extremos de la série indicada, tales como ma y $(k-m)a$, producen, fuera del signo, restos iguales (mod. k). Pero de todos modos, la resolucion sería enojosa siempre que el módulo y el coeficiente de la incógnita, en la congruencia cuya solucion buscamos, fuesen números ya un poco grandes: por lo cual necesitamos apelar á otro método más sencillo.

69.—*Segundo método.*

Para explicar debidamente este método advertiremos ante todo que, sin menoscabo de la generalidad exigida en éste asunto, podemos concretarnos al caso en que el coeficiente de la incógnita y el módulo sean primos entre sí, y además igual á la unidad el segundo miembro; porque evidentemente, si designamos por r la raiz de la congruencia

$$ax \equiv \pm 1,$$

será $\pm br$ la de la congruencia

$$ax \equiv \pm b.$$

Llamando b al módulo, para que sea mas completa la semejanza entre esta notacion y la que se acostumbra en los libros de Algebra, nuestro problema se reduce á resolver la congruencia

$$ax \equiv \pm 1 \text{ (mod. } b),$$

ó, si se quiere, la ecuacion indeterminada de primer grado

$$ax - by = \pm 1.$$

Para efectuarlo hallaremos el máximo comun divisor del coeficiente a

y el módulo b, y obtendremos (40) el sistema de igualdades:

$$a = \gamma\, b + c$$
$$b = \delta\, c + d$$
$$\cdots\cdots\cdots$$
$$l = \nu m + 1 :$$
$$m = m\,1 + 0.$$

Con los cocientes resultantes de este algoritmo, incluso el de la última division cuyo resto es cero, formemos la fraccion contínua

$$\gamma + \cfrac{1}{\delta + \cfrac{1}{\varepsilon + \vdots + \cfrac{1}{\lambda + \cfrac{1}{\mu + \cfrac{1}{\nu + \cfrac{1}{m}}}}}} = (\gamma, \delta, \varepsilon \ldots\ldots \lambda, \mu, \nu, m$$

Si las reducidas de esta fraccion contínua, á saber:

$$\frac{\gamma}{1}; \quad \gamma + \frac{1}{\delta} = \frac{\gamma\delta + 1}{\delta}; \quad \gamma + \frac{1}{\delta + \frac{1}{\varepsilon}} = \frac{(\gamma\delta + 1)\varepsilon + \gamma}{\delta\varepsilon + 1}; \quad \text{etc.}$$

las representamos por los símbolos

$$\frac{[\gamma]}{1}; \quad \frac{[\gamma, \delta]}{[\delta]}; \quad \frac{[\gamma, \delta, \varepsilon]}{[\delta, \varepsilon]}; \quad \text{etc..}$$

la diferencia entre la última y la penúltima, segun una ley conocida *), será:

$$[\gamma, \delta \ldots\ldots \nu, m]\,[\delta \ldots\ldots \nu] - [\delta \ldots\ldots \nu, m]\,[\gamma, \delta \ldots\ldots \nu] = \pm 1$$

*) Apéndice I.

en la cual se tomará el signo + ó el — segun que el número de los cocientes γ, δ, ε, ... μ, ν, m sea par ó impar.

Pero los dos términos de la última reducida son iguales respectivamente á los de la fraccion generatriz de la contínua, $\frac{a}{b}$, esto es:

$$[\gamma, \delta, \varepsilon, \ldots\ldots \mu, \nu, m] = a \quad \text{y} \quad [\delta, \varepsilon, \ldots\ldots \mu, \nu, m] = b:$$

luego, sustituyendo estos valores en la igualdad anterior, se convierte en la siguiente:

$$a\,[\delta, \varepsilon, \ldots\ldots \mu, \nu] - b\,[\gamma, \delta, \ldots\ldots \mu, \nu] = \pm 1,$$

que equivale á la congruencia,

$$a\,[\delta, \varepsilon, \ldots\ldots \mu, \nu] \equiv \pm 1 \pmod{b}:$$

de donde se deduce que los valores de x é y que buscamos son, prescindiendo del signo, iguales respectivamente al denominador y al numerador de la penúltima reducida. Y, como respecto de los signos, ya indicamos antes la regla que debe seguirse, la cuestion está completamente terminada.

Hallada por este procedimiento una solucion cualquiera (x', y'), el problema está completamente resuelto; porque de las igualdades

$$ax - by = 1 = ax' - by'$$

se deduce esta otra:

$$a(x - x') - b(y - y');$$

la cual exige, como a y b son primos entre sí, que $(x - x')$ sea divisible por b, y que $y - y'$ lo sea por a. Llamando z al cociente comun, tendremos las formas

$$x = x' + bz, \quad y = y' + az$$

que representan todos los pares de soluciones de la ecuacion propuesta, si z recibe sucesivamente los valores de la série numérica entera.

Ejemplo. Sea la congruencia

$$37x \equiv 1 \pmod{100}.$$

El algoritmo del máximo comun divisor (40) de los números 37 y 100 se expresará como sigue:

100	37	0						$37 = 0 \cdot 100 + 37$
	0							
37	100	2						$100 = 2 \cdot 37 + 26$
	74							
26	37	1						$37 = 1 \cdot 26 + 11$
	26							
11	26	2						$26 = 2 \cdot 11 + 4$
	22							
4	11	2						$11 = 2 \cdot 4 + 3$
	8							
3	4	1						$4 = 1 \cdot 3 + 1$
	3							
	1							$3 = 3 \cdot 1$

Los cocientes resultantes de este algoritmo son:

$$0,\ 2,\ 1,\ 2,\ 2,\ 1,\ 3.$$

Para calcular las reducidas tendremos:

0	2	1	2	2	1	3
$\frac{0}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{3}{8}$	$\frac{7}{19}$	$\frac{10}{27}$	$\frac{37}{100}$

y, teniendo en cuenta que el número de los cocientes expresados es impar, se desprende inmediatamente que:

$$x \equiv -27 \equiv 73 \pmod{100}$$

$$y \equiv -10 \pmod{37}$$

ó bien

$$x = -27 + 100z \quad \text{é} \quad y = -10 + 37z.$$

Haciendo la comprobacion se encuentra efectivamente:

$$37 \cdot (-27) - 100 \cdot (-10) = 1.$$

Para resolver la congruencia dada

$$37x \equiv 1 \text{ (mod. } 100)$$

por el método primero hubiéramos tenido que elevar el número 37 á la potencia

$$\varphi(100) - 1 = 39:$$

operacion más embarazosa y expuesta á equivocaciones que la del máximo comun divisor de los números 37 y 100, y consiguientes ahora explicadas.

Escólio. De un modo semejante á lo que se hace en las ecuaciones, podemos aquí tambien expresar la raiz de la congruencia

$$ax \equiv b \text{ (mod. } k)$$

por $\frac{b}{a}$ (mod. k). Así, por ejemplo, $\frac{1}{37}$ (mod. 100) representará todo número

$$\equiv -27 \equiv 73 \text{ (mod. } 100).$$

Esta expresion $\frac{b}{a}$ (mod. k), como sabemos, no significará nada real, si los números a y k contienen algun factor comun por el cual no sea tambien b divisible; pero, fuera de este caso, la raiz $\frac{b}{a}$ (mod. k) tendrá valores reales en número infinito: congruentes segun k, siempre que a y k sean primos entre sí, ó congruentes, segun $\frac{k}{\delta} = k'$, cuando δ represente el máximo comun divisor de dichos números, a y k. Por consecuencia, siempre que existan dos múltiplos cualesquiera, ax y bx, que se diferencien en la unidad, de los números a y b, éstos números serán primos entre sí; y, dados estos números, primos entre sí, siempre será posible encontrar pares, en número infinito, de otros números (x, y), que satisfagan á la ecuacion

$$ax - by = 1.$$

De estos principios se desprende la importante proposicion siguiente

70.—*Demostracion de la fórmula* $ax + by + cz + \ldots = \delta$, *donde* δ *representa el máximo comun divisor de los números* a, b, c.....

Designando por δ *el máximo comun divisor de varios números* a, b, c, d..... *siempre será posible determinar otros tantos números* x, y, z, u....., *de modo que se verifique, entre los primeros y los segundos, la ecuacion*

$$ax + by + cz + du + \ldots = \delta.$$

En efecto, consideremos primeramente dos números nada más, a y b, y llamemos δ' á su máximo comun divisor: entónces la congruencia

$$ax \equiv \delta' \pmod{b}$$

será posible. Designando por x' su raiz, y haciendo

$$\frac{\delta' - ax'}{b} = y'.$$

tendremos, conforme al enunciado del teorema, la relacion

$$ax' + by' = \delta'.$$

Representando ahora por δ'' el máximo comun divisor de δ' y c, ó, lo que es igual (42), el máximo comun divisor de los tres números a, b, c, se determinarán, como antes, dos nuevos números, x'', y'', que satisfarán á la ecuacion

$$\delta' x'' + cy'' = \delta'';$$

de la cual, sustituyendo por δ' su valor hallado, se deduce esta otra:

$$ax'x'' + by'x'' + cy'' = \delta''.$$

Significando por δ''' el máximo comun divisor de δ'' y d, ó bien, el máximo comun divisor de los cuatro números a, b, c, d, determi-

naremos tambien otro par de números x''', y''', ligados por la relacion

$$b''x''' + dy''' = b''',$$

que se convertirá en la siguiente:

$$ax'x''x''' + by'x''x''' + cy''x''' + dy''' = b'''$$

y así continuaríamos, fuesen cuantos quisieran los números $a, b, c, d.....$

Si estos números $a, b, c, d.....$ fuesen primos entre sí, su máximo comun divisor sería la unidad (42-Cor.), y la relacion entre ellos

$$ax + by + cz + ... = 1.$$

Nótese que, siendo dos los números, a y b, tenemos las igualdades

$$x = x' \qquad y = y';$$

siendo tres, a, b, c, estas otras:

$$x = x'x'', \qquad y = y'x''. \qquad z = y'';$$

y, siendo cuatro, a, b, c, d, las que siguen:

$$x = x'x''x''', \qquad y = y'x''x''', \qquad z = y''x''', \qquad u = y''';$$

cuya ley de formacion es patente.

La resolucion de las congruencias de primer grado es el fundamento para la de muchos problemas, entre los cuales debemos estudiar, por su importancia, los siguientes:

71.—*Hallar los números congruentes con dos números dados, respecto de dos módulos dados.*

Sean estos módulos A, B, segun los cuales un número x debe ser *cóngruo* respectivamente á los determinados a y b. Este número x debe satisfacer, por consiguiente, á las dos congruencias

$$x \equiv a \text{ (mod. } A)$$

$$x \equiv b \text{ (mod. } B)$$

por satisfacer á la primera tendrá la forma

$$x = a + Az$$

la cual, sustituida en la segunda, nos dará esta otra

$$Az \equiv b - a \text{ (mod. } B) \qquad (1)$$

para determinar el valor de la nueva incógnita z.

Ahora bien, si designamos por δ el máximo comun divisor de los módulos A, B, esta congruencia será posible (68-2.°) siempre que su segundo miembro $b - a$ sea divisible por δ, ó, únicamente, cuando se verifique la congruencia

$$a \equiv b \text{ (mod. } \delta) \qquad (2)$$

Cumplida esta condicion, la solucion completa de la congruencia (1) será, como sabemos

$$z \equiv v \left(\text{mod. } \frac{B}{\delta} \right), \text{ ó bien, } z = v + \frac{B}{\delta} n$$

en cuya forma representa v una raiz cualquiera de dicha congruencia y n un número entero arbitrario. Sustituyendo este valor de z en el de x obtendremos, por fin, la forma

$$x = a + Av + \frac{AB}{\delta} n$$

de todos los números x que reunen las condiciones exigidas en el enunciado del problema; y la cual, haciendo

$$a + Av = x_0,$$

puede tambien expresarse del modo siguiente:

$$x \equiv x_0 \left(\text{mod. } \frac{AB}{\delta} \right).$$

Ejemplo. Hallar los números que divididos por 12 produzcan el resto 7, y divididos por 15 den el resto 4, es decir, resolver las congruencias

$$x \equiv 7 \text{ (mod. 12)} \quad \text{y} \quad x \equiv 4 \text{ (mod. 15)}.$$

Haciendo

$$x = 7 + 12z,$$

y sustituyendo este valor de x en la segunda congruencia, obtendremos la siguiente:

$$12z \equiv -3 \pmod{15},$$

que satisface á la condicion necesaria (2) para ser posible; puesto que su segundo miembro, -3, es divisible por el máximo comun divisor, 3, de los módulos 12 y 15. Simplificándola, pues, se convierte en esta otra:

$$4z \equiv -1 \pmod{5}.$$

cuya solucion completa es

$$z \equiv 1 \pmod{5}, \quad \text{ó bien}, \quad z = 1 + 5n;$$

de la cual se deduce

$$x = 7 + 12 + 60n, \quad \text{ó bien} \quad x \equiv 19 \pmod{60}.$$

72.—*Hallar los números congruentes con varios números dados respecto de vários módulos dados.*

Si agregásemos un tercer módulo C, segun el cual fuesen los números x cóngruos con c, procederíamos del mismo modo; y, designando por δ' el máximo comun divisor de los números

$$\frac{AB}{\delta} \quad \text{y} \quad C, \quad \text{y por} \quad z' \equiv v' \left(\text{mod.} \ \frac{C}{\delta'} \right)$$

la raiz de la congruencia

$$\frac{AB}{\delta} z' + Av + a \equiv c \pmod{C},$$

la solucion completa de la cuestion sería entónces:

$$x \equiv \frac{AB}{\delta} v' + Av + a \left(\text{mod. } \frac{ABC}{\delta\delta'} \right)$$

Y análogas soluciones se encontrarían, si en vez de ser de tres, fuesen cuatro ó más los módulos propuestos.

Adviértase que los números

$$\frac{AB}{\delta} \; ; \quad \frac{ABC}{\delta\delta'}$$

son los mínimos múltiplos comunes (44) de los módulos

$$A.\ B. \qquad A.\ B.\ C.$$

respectivamente: así que, si M representa este mínimo comun múltiplo, la solucion completa de las congruencias de un mismo número x, referido á varios módulos A, B, C..... tendria, en último resultado, la forma

$$x \equiv r \text{ (mod. } M).$$

Mas si estos módulos fuesen primos entre sí dos á dos, la condicion (2) se cumpliria siempre, y sería su producto su mínimo comun múltiplo (44-Cor.), dependiendo entónces la resolucion de las congruencias,

$$x \equiv a \text{ (mod. } A), \qquad x \equiv b \text{ (mod. } B), \qquad x \equiv c \text{ (mod. } C) \ldots\ldots,$$

de la congruencia única

$$x \equiv r \text{ (mod. } P).$$

siendo

$$P = ABC\ldots\ldots$$

Recíprocamente, esta única congruencia puede resolverse en las anteriores, descomponiendo el número P en sus factores primos.

Infiérese de lo dicho que el problema de verdadera importancia, y de utilidad para nosotros, será aquél en que se supongan los módulos primos entre sí dos á dos, y cuyo enunciado es:

Hallar los números x que satisfagan al sistema de congruencias

$$x \equiv a \text{ (mod. } A)$$

$$x \equiv b \text{ (mod. } B)$$

$$x \equiv c \text{ (mod. } C)$$

$$x \equiv d \text{ (mod. } D)$$

. . . . . .

en las cuales representan los módulos

$$A,\ B,\ C,\ D\ldots\ldots,$$

números primos entre sí dos á dos.

El procedimiento para resolver este problema queda ya anteriormente indicado; mas, en lugar de buscar por operaciones sucesivas, segun se dijo, la solucion pedida, se puede hallar con ménos embarazo por otro método que á continuacion se explica.

Distribuyamos el producto

$$P = A\,B\,C\,D\ldots\ldots$$

de los módulos en dos factores, como sigue:

$$P = A\,.\,(B\,C\,D\ldots\ldots) = B\,.\,(A\,C\,D\ldots\ldots) = C\,.\,(A\,B\,D\ldots\ldots)$$
$$= D\,.\,(A\,B\,C\ldots\ldots) = \ldots\ldots$$

y, para mayor brevedad, hagamos

$$P = A\,.\,A' = B\,.\,B' = C\,.\,C' = D\,.\,D' = \ldots\ldots$$

Determínense ahora los números α, β, γ..... que satisfagan respectivamente á las congruencias

$$A'\alpha \equiv 1 \text{ (mod. } A), \qquad B'\beta \equiv 1 \text{ (mod. } B), \qquad C'\gamma \equiv 1 \text{ (mod. } C), \ldots\ldots$$

y los números x que se buscan estarán dados por la congruencia

$$x \equiv A'\alpha\,a + B'\beta\,b + C'\gamma\,c + \ldots\ldots \text{ (mod. } P):$$

puesto que de la congruencia

$$A'\alpha \equiv 1 \text{ (mod. } A)$$

se deduce esta otra

$$A'\alpha a \equiv a \text{ (mod. } A);$$

la cual prueba que el primer término en el valor de x es realmente congruente con a (mod. A), mientras que los otros términos son nulos respecto de A; y lo mismo puede demostrarse para cada uno de los términos

$$B'\beta b, \quad C'\gamma c \ldots\ldots$$

que son congruentes con b (mod. B), c (mod. C)..... al tiempo que todos los demás son, en cada caso, nulos, segun los módulos respectivos.

Además de su brevedad posee este método la ventaja de que los números auxiliares, α, β, γ....., determinados mediante los módulos exclusivamente, permanecen constantes para cualesquiera restos, mientras dichos módulos no varien.

Escólio. La congruencia

$$x \equiv r \text{ (mod. } P),$$

donde se supone

$$r \quad A'\alpha a + B'\beta b + C'\gamma c + \ldots\ldots$$

representa todos los números que satisfacen á las condiciones del problema y son congruentes con r (mod. P); mas, como los restos que cualquiera de ellos produce al ser divididos sucesivamente por los factores A, B, C..... de P, son tambien congruentes con r (61–7.ª) segun cada uno de estos divisores, resulta que estos restos y los de los números x coinciden, esto es, son los mismos restos dados, a, b, c..... Si, pues, cada uno de estos números a, b, c..... recibe los valores de un sistema completo de restos (62) segun los módulos A, B, C..... respectivamente, la expresion anterior de x tomará del mismo modo los valores de un sistema completo de restos segun el módulo

$$P = ABC\ldots.$$

Es evidente que los restos a, b, c..... pueden recibir, así como se

ha dicho, A, B, C..... valores distintos respectivamente, y al resto r corresponderán

$$P - ABC.....$$

valores; pero en el caso de ser los números a, b, c....., primos con sus módulos, solo podrán tener

$$\varphi(A), \quad \varphi(B), \quad \varphi(C).....$$

valores, y

$$\varphi(P) = \varphi(ABC.....)$$

el número x; y como este último número de los valores de x tiene que ser igual al producto de los valores respectivos de los restos a, b, c....., resulta nuevamente la relacion (56)

$$\varphi(ABC.....) = \varphi(A)\,\varphi(B)\,\varphi(C).....$$

Esta conclusion nos proporciona á su vez un nuevo medio para determinar la forma explícita de la funcion φ (*).

En efecto: si N es un número primo a, el número de los términos de la série

$$1, \quad 2, \quad 3..... \quad a$$

primos con a, será evidentemente

$$\varphi(a) = a - 1.$$

Si $N = a^{\alpha}$, los términos de la série

$$1, \quad 2, \quad 3..... \quad a^{\alpha}.$$

divisibles por a, se hallarán todos comprendidos en esta otra:

$$a, \quad 2a, \quad 3a..... \quad a^{\alpha-1}.a,$$

que consta de $a^{\alpha-1}$ términos: luego restando de los a^{α} términos de la série anterior los $a^{\alpha-1}$ de esta última, la diferencia

---

(*) *Euleri* comm. arithm. XX—16. *Serret*, Cours d'Algèbre supérieure, §. 285.

$$a^{\alpha} - a^{\alpha-1} = a^{\alpha}\left(1 - \frac{1}{a}\right)$$

expresará el número de los números primos con el propuesto a^{α}, é inferiores al mismo. Y, finalmente, si N es un número primo cualquiera,

$$N = a^{\alpha}\, b^{\beta}\, c^{\gamma} \ldots\ldots$$

tendremos por una parte:

$$\varphi(N) = (a^{\alpha})\,\varphi(b^{\beta})\,\varphi(c^{\gamma})\ldots\ldots$$

y por otra:

$$\varphi(a^{\alpha}) = a^{\alpha}\left(1 - \frac{1}{a}\right)$$

$$\varphi(b^{\beta}) \quad b^{\beta}\left(1 - \frac{1}{b}\right)$$

$$\varphi(c^{\gamma}) = c^{\gamma}\left(1 - \frac{1}{c}\right)$$

de cuyas igualdades resulta la siguiente:

$$\varphi(N) = N\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\left(1 - \frac{1}{c}\right)\ldots\ldots$$

que representa el valor de la funcion φ.

Ejemplo. Hallar los números que divididos por 3, 7, 10, produzcan respectivamente los restos 2, 3, 9.

En este caso tendremos:

$$P = 3 \,.\, 7 \,.\, 10 = 3 \,.\, 70 - 7 \,.\, 30 - 10 \,.\, 21$$

y, por consiguiente, las congruencias

$$\begin{array}{lll} 70\,\alpha \equiv 1 \pmod{3} & & \alpha \equiv 1 \pmod{3} \\ 30\,\beta \equiv 1 \pmod{7} & \text{que dan:} & \beta \equiv 4 \pmod{7} \\ 21\,\gamma \equiv 1 \pmod{10} & & \gamma \equiv 1 \pmod{10}\,; \end{array}$$

de donde resulta, por fin.

$$x \equiv 70 \,.\, 1 \,.\, 2 + 30 \,.\, 4 \,.\, 3 + 21 \,.\, 1 \,.\, 9 = 689 \equiv 59 \text{ (mod. } 210).$$

Para enseñar prácticamente cómo se debe proceder cuando los módulos dados no sean primos, y las precauciones que en este caso conviene tomar para reducirlo al anterior, resolverèmos á continuacion otro ejemplo.

Sean los módulos y restos dados respectivamente

$$A = 6, \quad B = 12, \quad C = 15,$$
$$a = 1, \quad b = 1, \quad c = 10.$$

Desde luego podremos prescindir del módulo 6; puesto que si un número es congruente con la unidad segun el módulo 12, lo será tambien segun el módulo 6. Por otra parte, todo número $\equiv 1$ (mod. 12) debe tener la forma

$$3 \,.\, 4\, n + 1:$$

la cual manifiesta que dicho número tambien dará el resto 1 segun los módulos 3 y 4; y todo número $\equiv 10$ (mod. 15) afectará la forma

$$3 \,.\, 5\, n + 10,$$

que, dividida por 3, produce asimismo el resto 1, y el resto 0 si se divide por 5. Luego los datos del problema propuesto se convierten, sin menoscabo de su significacion primitiva, en estos otros:

$$A = 3, \quad B = 4, \quad C = 5,$$
$$a = 1, \quad b = 1, \quad c = 0,$$

que cumplen ya con las condiciones exigidas á los del primer problema.

Las congruencias, pues, para resolver el actual serán:

$$20\,\alpha \equiv 1 \text{ (mod. } 3) \qquad \alpha \equiv 2 \text{ (mod. } 3)$$
$$15\,\beta \equiv 1 \text{ (mod. } 4) \quad \text{de donde se deducen:} \quad \beta \equiv 3 \text{ (mod. } 4)$$
$$12\,\gamma \equiv 1 \text{ (mod. } 5) \qquad \gamma \equiv 3 \text{ (mod. } 5)$$

y, por consecuencia, la congruencia final

$$x \equiv 20 \,.\, 2 \,.\, 1 + 15 \,.\, 3 \,.\, 1 + 12 \,.\, 3 \,.\, 0 = 85 \equiv 25 \,(\text{mod. } 60),$$

que patentiza ser

$$x = 25 + 60\,z$$

la forma de los números x que se buscaban.

73.—*Descomposicion de una fraccion en la suma de otras más sencillas.*

Si escribimos en forma de ecuacion la congruencia

$$x \equiv A'\alpha\, a + B'\beta\, a + C'\gamma\, c + \cdots\cdots \,(\text{mod. } P),$$

tendremos:

$$x = n\,P + A'\alpha\, a + B'\beta\, b + C'\gamma\, c + \cdots\cdots$$

ó bien, dividiendo por

$$P = A\,B\,C\ldots\ldots = A \,.\, A' = B \,.\, B' = C \,.\, C' = \ldots\ldots$$

$$\frac{x}{P} = n + \frac{\alpha\, a}{A} + \frac{\beta\, a}{B} + \frac{\gamma\, c}{C} + \cdots\cdots$$

en cuya expresion los números

$$n, \quad \alpha\, a, \quad \beta\, b, \quad \gamma\, c\ldots\ldots$$

representan, como sabemos, números enteros.

Si designamos, pues, por N un número entero cualquiera, hacemos, como antes,

$$P = A\,B\,C\ldots\ldots,$$

y establecemos la igualdad

$$\frac{N}{P} = n + \frac{x}{A} + \frac{y}{B} + \frac{z}{C} + \ldots\ldots$$

se deducirá esta otra:

$$N = nP + A'x + B'y + C'z + \ldots\ldots$$

y las congruencias para determinar los numeradores x, y, z..... serán evidentemente:

$$N \equiv A'x \text{ (mod. } A)$$

$$N \equiv B'y \text{ (mod. } B)$$

$$N \equiv C'z \text{ (mod. } C)$$

. . . . . .

en las cuales figurará tal cual sea el mismo número N dado, siempre que sea $P > N$, y por tanto, $n = 0$; ó bien el resto resultante de dividir N por P, cuando la fraccion $N : P$ sea impropia.

Ejemplo. Sea la fraccion

$$\frac{N}{P} = \frac{523}{840};$$

descompondremos su denominador en sus factores primos entre sí dos á dos

$$3, \quad 5, \quad 7, \quad 8,$$

y tendremos, por consecuencia:

$$\frac{523}{840} = \frac{x}{3} + \frac{y}{5} + \frac{z}{7} + \frac{u}{8}$$

y tambien

$$A = 3 \qquad A' = 280$$

$$B = 5 \qquad B' = 168$$

$$C = 7 \qquad C' = 120$$

$$D = 8 \qquad D' = 105$$

Con estos datos las congruencias para determinar los numeradores

$$x, \quad y, \quad z, \quad u$$

serán estas:

$$280\,x \equiv 523 \text{ (mod. 3)}$$

$$168\,y \equiv 523 \text{ (mod. 5)}$$

$$120\,z \equiv 523 \text{ (mod. 7)}$$

$$105\,u \equiv 523 \text{ (mod. 8)}$$

De las cuales, dividiendo sus dos miembros por el módulo respectivo, y tomando los restos mínimos absolutos, se deducen las soluciones

$$x \equiv 1 \text{ (mod. 3)}$$

$$y \equiv 1 \text{ (mod. 5)}$$

$$z \equiv 2 \text{ (mod. 7)}$$

$$u \equiv 3 \text{ (mod. 8)}$$

Y de aquí la descomposicion que se deseaba:

$$\frac{523}{840} = \frac{1}{3} + \frac{1}{5} - \frac{2}{7} + \frac{3}{8} = \frac{280 + 168 - 240 + 315}{840}.$$

Es claro que, admitiendo cada una de las últimas congruencias infinidad de valores congruentes, el número de soluciones para el problema propuesto es tambien ilimitado, pero se limitará desde el momento que se imponga á las fracciones parciales que se buscan la condicion de ser propias. Quitando una unidad al último quebrado $\frac{3}{8}$ y agregándosela al penúltimo $-\frac{2}{7}$ resulta la nueva descomposicion

$$\frac{523}{840} = \frac{1}{3} + \frac{1}{5} + \frac{5}{7} - \frac{5}{8};$$

Agregando una unidad al quebrado $-\frac{2}{7}$, y quitándosela, bien al quebrado $\frac{1}{5}$, bien á $\frac{1}{3}$, tendremos otras dos descomposiciones, á saber:

$$\frac{523}{840} = \frac{1}{3} - \frac{1}{5} + \frac{5}{7} + \frac{3}{8}$$

$$\frac{523}{840} = \frac{2}{3} + \frac{1}{5} + \frac{5}{7} + \frac{3}{8}$$

que completan las cuatro posibles en el caso particular de que tratamos.

74.—*Resolucion de varias congruencias de primer grado con igual número de incógnitas.*

Sean las congruencias (*)

$$\left.\begin{aligned} a\,x + b\,y + c\,z + \cdots\cdots &\equiv f \\ a'\,x + b'\,y + c'\,z + \cdots\cdots &\equiv f' \\ a''x + b''y + c''z + \cdots\cdots &\equiv f'' \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots & \end{aligned}\right\} \pmod{k} \qquad (A)$$

cuyo número supondremos igual á n.

Multiplicando respectivamente estas congruencias por los factores indeterminados ξ, ξ', ξ''....., sumándolas despues ordenadamente, é igualando á cero los coeficientes de cada una de las incógnitas, excepto la x, obtendremos las $(n-1)$ ecuaciones,

$$\begin{aligned} b\xi + b'\xi' + b''\xi'' + \cdots\cdots &= 0 \\ c\xi + c'\xi' + c''\xi'' + \cdots\cdots &= 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots & \end{aligned}$$

mediante las cuales podrán determinarse los $(n-1)$ cocientes

$$\frac{\xi'}{\xi}, \quad \frac{\xi''}{\xi}, \quad \frac{\xi'''}{\xi}, \quad \frac{\xi^{IV}}{\xi}, \ldots\ldots$$

(*) *Gauss.*—D. A. §. 37.

á cuyo fin se tomarán los valores ξ de modo que ξ, ξ', ξ'', ξ'''..... sean primos entre sí dos á dos.

Eliminadas así todas las incógnitas, ménos la x, la congruencia resultante contendrá solamente esta última, representando en ella las letras ξ números enteros.

Aplicando el mismo método de eliminacion para todas las incógnitas, excepto la y, obtendremos un nuevo sistema de $(n-1)$ ecuaciones, semejante al anterior,

$$a\eta + a'\eta' + a''\eta'' + \cdots\cdots = 0$$

$$c\eta + c'\eta' + c''\eta'' + \cdots\cdots = 0$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

para determinar los números η, η', η'', ... con la condicion de ser tambien primos entre sí, como los ξ, ξ', ξ''.....

La congruencia resultante, en este caso, contendrá solamente la incógnita y y las cantidades η, η', η''..... ya determinadas.

De un modo semejante llegaremos á otra congruencia con la incógnita z y los números ζ, determinados por el sistema de ecuaciones

$$a\zeta + a'\zeta' + a''\zeta'' + \cdots\cdots = 0$$

$$b\zeta + b'\zeta' + b''\zeta'' + \cdots\cdots = 0$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

Y, repitiendo el mismo procedimiento, es evidente que de las n congruencias dadas acabaremos por deducir otras tantas en cada una de las cuales figure una sola incógnita, á saber:

$$\left.\begin{array}{l} (a\xi + a'\xi' + a''\xi'' + \ldots..)x \equiv f\xi + f'\xi' + f''\xi'' + \cdots\cdots \\ (b\eta + b'\eta' + b''\eta'' + \ldots..)y \equiv f\eta + f'\eta' + f''\eta'' + \cdots\cdots \\ (c\zeta + c'\zeta' + c''\zeta'' + \ldots..)z \equiv f\zeta + f'\zeta' + f''\zeta'' + \cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{array}\right\} (\text{mod. } k)$$

las cuales pueden escribirse abreviadamente de este modo:

$$\left.\begin{aligned} x\Sigma a\xi &\equiv \Sigma f\xi \\ y\Sigma b\eta &\equiv \Sigma f\eta \\ z\Sigma c\zeta &\equiv \Sigma f\zeta \\ &\cdots\cdots\cdots \end{aligned}\right\} \text{(mod. } k\text{)} \qquad - \quad (B)$$

La resolucion de varias congruencias con varias incógnitas, por consecuencia, se reduce á la de varias congruencias cada una de las cuales contiene una sola incógnita: problema que ya sabemos resolver.

Mas conviene, sin embargo, recordar algunas ideas y examinar aquí tambien los dos casos que en su lugar oportuno (68) consideramos.

1.° Cuando todos los coeficientes $\Sigma a\xi$, $\Sigma b\eta$, ... de las incógnitas son primos con el módulo k, las congruencias correspondientes son posibles (1.°) y la solucion completa del problema se expresará por congruencias de la forma $x \equiv p \text{(mod. } k\text{)}$, $y \equiv q \text{(mod. } k\text{)}$..... etc.

Así, por ejemplo, si se dan las congruencias

$$\left.\begin{aligned} x + 3y + z &\equiv 1 \\ 4x + y + 5z &\equiv 7 \\ 2x + 2y + z &\equiv 3 \end{aligned}\right\} \text{(mod. } 8\text{)}$$

se hallan facilmente $\xi = 9$, $\xi' = 1$, $\xi'' = -14$; y, por consecuencia, $-15x \equiv -26$ y de aquí $x \equiv 6 \text{(mod. } 8\text{)}$. Del mismo modo se encuentran las congruencias $15y \equiv -4$, $15z \equiv 1$, y sus raices correspondientes $y \equiv 4$, $z \equiv 7 \text{(mod. } 8\text{)}$.

2.° Si los coeficientes $\Sigma a\xi$, $\Sigma b\eta$, $\Sigma c\zeta$..... no son todos primos con el módulo k, y designamos por δ, δ', δ''..... los máximos comunes divisores de este módulo y de los números $\Sigma a\xi$, $\Sigma b\eta$, $\Sigma c\zeta$,..... respectivamente, el problema será imposible siempre que dichos divisores no dividan tambien en cada caso á los segundos miembros $\Sigma f\xi$, $\Sigma f\eta$, $\Sigma c\zeta$..... Pero, si esta condicion se cumple, el sistema de congruencias (B) será posible y su solucion estará expresada por congruencias de las formas

$$x \equiv p\left(\text{mod. } \frac{k}{\delta}\right), \quad y \equiv q\left(\text{mod. } \frac{k}{\delta'}\right), \quad z \equiv r\left(\text{mod. } \frac{k}{\delta''}\right) \cdots\cdots$$

las cuales darán δ valores incongruentes (mod. k) para x, δ' valores diferentes para y, δ'' para z..... etc., que satisfarán tambien á las del sistema mencionado. Mas conviene advertir que, si bien todas las soluciones de las congruencias propuestas (A) se hallan entre las δ, δ' δ''..... etc., de las últimas, no todas las combinaciones de todos los δ valores de x, con todos los δ' de y, con todos los δ'' de z..... etc., satisfarán tambien al problema de cuya resolucion tratamos, sino solamente algunas ligadas entre sí mediante ciertas congruencias de condicion (68–2.°).

Para mayor esclarecimiento de estas ideas resolveremos minuciosamente el siguiente

Ejemplo. Sean las congruencias

$$\left.\begin{aligned} 3x+5y+\ z &\equiv 4 \\ 2x+3y+2z &\equiv 7 \\ 5x+\ y+3z &\equiv 6 \end{aligned}\right\} (\text{mod. } 12)$$

Las ecuaciones para determinar los cocientes

$$\frac{\xi'}{\xi},\ \frac{\xi''}{\xi},\ \frac{\xi'''}{\xi}\ldots\ldots,\quad \frac{\eta'}{\eta},\ \frac{\eta''}{\eta},\ \frac{\eta'''}{\eta}\ldots\ldots,\quad \frac{\zeta'}{\zeta},\ \frac{\zeta''}{\zeta},\ \frac{\zeta'''}{\zeta}\ldots\ldots$$

son:

$$\left.\begin{aligned} 5\xi+3\xi'+\ \xi'' &= 0 \\ \xi+2\xi'+3\xi'' &= 0 \end{aligned}\right\} \text{para los } \xi$$

$$\left.\begin{aligned} 3\eta+2\eta'+5\eta'' &= 0 \\ \eta+2\eta'+3\eta'' &= 0 \end{aligned}\right\} \text{para los } \eta$$

$$\left.\begin{aligned} 3\zeta+2\zeta'+5\zeta'' &= 0 \\ 5\zeta+3\zeta'+\ \zeta'' &= 0 \end{aligned}\right\} \text{para los } \zeta$$

de los cuales se deduce:

$$\begin{array}{lll} \xi = 1 & \eta = 1 & \zeta = -13 \\ \xi' = -2 & \eta' = 1 & \zeta' = 22 \\ \xi'' = 1 & \eta'' = -1 & \zeta'' = -1 \end{array}$$

Teniendo presente que en este caso particular son:

$$\begin{array}{llll} a = 3 & b = 5 & c = 1 & f = 4 \\ a' = 2 & b' = 2 & c' = 2 & f' = 7 \\ a'' = 5 & b'' = 1 & c'' = 3 & f'' = 6 \end{array}$$

facilmente hallaremos:

$$\begin{array}{llll} \Sigma a\xi = & 3 - 4 + 5 = 4 & \Sigma f\xi = & 4 - 14 + 6 = -4 \\ \Sigma b\eta = & 5 + 3 - 1 = 7 & \Sigma f\eta = & 4 + 7 - 6 = 5 \\ \Sigma c\zeta = & -13 + 44 - 3 = 28 & \Sigma f\zeta = & -52 + 154 - 6 = 96 \end{array}$$

Por consecuencia, el sistema de congruencias que tenemos que resolver es el siguiente:

$$\left.\begin{array}{rl} 4x \equiv & -4 \\ 7y \equiv & 5 \\ 28z \equiv & 96 \end{array}\right\} \text{(mod. 12)}$$

ó bien (61-5.ª) este otro:

$$\begin{array}{rl} x \equiv & -1 \text{ (mod. 3)} \\ 7y \equiv & 5 \text{ (mod. 12)} \\ 7z \equiv & 24 \text{ (mod. 3)} \end{array}$$

que se deduce del anterior dividiendo las congruencias primera y tercera por 4, máximo comun divisor de los coeficientes 4 y 28, y del módulo 12.

Estas últimas congruencias quedarán satisfechas por los valores representados en las que siguen

$$\begin{array}{rl} x \equiv & 2 \text{ (mod. 3)} \\ y \equiv & 11 \text{ (mod. 12)} \\ z \equiv & 0 \text{ (mod. 4)} \end{array}$$

ó bien (68-3.º) en estas otras

$$x \equiv 2,\ 5,\ 8,\ 11 \pmod 3$$
$$y \equiv 11 \equiv -1 \pmod{12}$$
$$z \equiv 0,\ 3,\ 6,\ 9 \pmod 3$$

Para hallar ahora las combinaciones de estos valores de x, y, z, que satisfacen al problema, sustituyamos en las congruencias dadas las formas

$$x = 2 + 3x', \qquad y = 11, \qquad z = 0 + 3z' = 3z'$$

y, despues de efectuada la trasposicion, obtendremos el nuevo sistema

$$\left.\begin{aligned} 57 + 9x' + 3z' &\equiv 0 \\ 30 + 6x' + 6z' &\equiv 0 \\ 15 + 15x' + 9z' &\equiv 0 \end{aligned}\right\} \pmod{12}$$

que, mediante la division por el comun divisor 3, se convierte (61–5.ª) en este otro:

$$\left.\begin{aligned} 19 + 3x' + z' &\equiv 0 \\ 10 + 2x' + 2z' &\equiv 0 \\ 5 + 6x' + 3z' &\equiv 0 \end{aligned}\right\} \pmod 4$$

ó bien, reduciendo todos los coeficientes á sus restos mínimos absolutos (mod. 4), en el siguiente:

$$\left.\begin{aligned} -(1 + x') + z' &\equiv 0 \\ 2(1 + x') + 2z' &\equiv 0 \\ (1 + x') + z' &\equiv 0 \end{aligned}\right\} \pmod 4$$

La primera y última de estas congruencias pueden reunirse en una sola, y la de enmedio expresa lo mismo que las otras dos, todavía de un modo más general, esto es, con referencia al módulo 2. Así que para evitar toda contradiccion estableceremos la congruencia condicional

$$z' \equiv (1 + x') \pmod 4;$$

de donde se desprende que, para obtener valores diferentes x y z, respecto del módulo 12, las cantidades x' y z' sólo pueden recibir los de la série 0, 1, 2, 3: los cuales, en virtud de la congruencia de condicion, producen exclusivamente las combinaciones posibles

$$\begin{array}{llll} x'=0 & x'=1 & x'=2 & x'=3 \\ z'=1 & z'=2 & z'=3 & z'=0. \end{array}$$

Dando, pues, á x' y z' en las formas $x=+3x'$, $z=3z'$, estos pares de valores, tendremos:

2, 5, 8, 11, para x:

3, 6, 9, 0, para los correspondientes de z.

Y de todo esto resulta que el problema propuesto admite las soluciones compatibles, siguientes:

$$\left.\begin{array}{l} x\equiv 2,\ 5,\ 8,\ 11 \\ y\equiv 11,\ 11,\ 11,\ 11 \\ z\equiv 3,\ 6,\ 9,\ 0 \end{array}\right\} (\text{mod. } 12).$$

CAPITULO II.

Proposiciones generales sobre las congruencias.

Ya dijimos (67) que dos funciones enteras y con coeficientes tambien enteros se llamaban congruentes, segun un módulo cualquiera, siempre que fuesen congruentes, respecto de este mismo módulo, los coeficientes respectivos de iguales potencias de su variable comun. Esta definicion es general; pero como las congruencias con módulos compuestos se refieren á otras de módulos primos, de cuya resolucion depende la de aquellas, nos concretaremos en cuanto vamos ahora á decir á los módulos primos solamente. Esto sentado, pasemos á demostrar las proposiciones que siguen.

75.—*Congruencia con cero del producto de dos funciones.*

Designando por p un número primo, el producto de dos funciones de x, enteras y con coeficientes enteros, $f(x)$ y $F(x)$, será congruente con CERO, *segun el módulo p, sólo cuando lo sea uno de sus factores.*

En efecto, siendo las funciones dadas

$$f(x) = a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n$$

$$F(x) = b_0 x^n + b_1 x^{n-1} + b_2 x^{n-2} + \cdots + b_{n-1} x + b_n .$$

para que ninguna de las dos sea $\equiv 0 \pmod{p}$ es necesario y suficiente que exista en cada una, por lo ménos, un coeficiente que no sea divisible por p. Designemos, pues, por a_{n-r} el primer coeficiente no divisible por p, contando desde el último, de la funcion $f(x)$; y por b_{n-s} el primer coeficiente de la funcion $F(x)$ que satisface tambien á las condiciones del anterior: de manera que todos los coeficientes, con índices superiores á estos dos, son divisibles por p en ambas funciones.

Esto supuesto, facilmente se ve que el coeficiente de la potencia x^{r-s} de la variable x, en el desarrollo del producto $f(x)F(x)$, es igual á

$$a_{n-r} \cdot b_{n-s} + a_{n-r+1} \cdot b_{n-s-1} + \cdots + b_{n-s+1} \cdot a_{n-s-1} + \cdots ,$$

esto es, igual á $a_{n-r} \cdot b_{n-s}$, más una série de términos que, segun la hipótesis, son todos múltiplos de p, de donde se deduce que tal coeficiente será

$$\equiv a_{n-r} \cdot b_{n-s} \pmod{p}.$$

Pero este producto, como el número p es primo, no es divisible por p, porque no lo es ninguno de sus factores; y, por consecuencia, tampoco serán divisibles por p todos los coeficientes de $f(x)F(x)$, como debieran serlo para que fuese $f(x)F(x) \equiv 0 \pmod{p}$: luego la suposicion de que ninguno de los factores $f(x)$, $F(x)$ sea $\equiv 0 \pmod{p}$ es inadmisible; resultando demostrado que la congruencia

$$f(x)\,F(x) \equiv 0 \,(\text{mod. } p)$$

exige que se verifique una de estas dos, por lo ménos:

$$f(x) \equiv 0 \,(\text{mod. } p)\,.$$

ó

$$F(x) \equiv 0 \,(\text{mod. } p)\,.$$

76.—*Descomposicion de una funcion entera en otras dos.*

En este teorema estriba la demostracion del siguiente, debido á Gauss (*).

Si una funcion entera con coeficientes enteros, de la forma

$$\varphi(x) = x^{m+n} + c_1 x^{m+n-1} + c_2 x^{m+n-2} + \cdots\cdots + c_{m+n-1}\,.\,x + c_{m+n}$$

no puede ser descompuesta en el producto de otras dos, tambien enteras y con coeficientes enteros,

$$f(x) = x^m + a_1 x^{m-1} + a_2 x^{m-2} + \cdots\cdots + a_{m-1}\,.\,x + a_m$$

$$F(x) = x^n + b_1 x^{n-2} + b_2 x^{n-2} + \cdots\cdots + b_{n-1}\,.\,x + b_n\,,$$

tampoco podrá ser descompuesta en el producto de dos funciones enteras, de la misma forma, con coeficientes racionales.

Admitamos, en efecto, que la funcion $\varphi(x)$ pueda ser descompuesta en el producto de dos funciones, $f(x)$, $F(x)$, enteras, con coeficientes racionales, pero fraccionarios: consideremos estos quebrados reducidos á comun denominador y designemos respectivamente por α y β los denominadores comunes de los coeficientes en $f(x)$ y $F(x)$.

Multiplicando cada una de estas funciones por su comun denominador, y estableciendo, para mayor sencillez, las igualdades generales,

---

(*) D. A., §. 42.

$$a_r = \frac{\alpha_r}{\gamma}, \quad b_r = \frac{\beta_r}{\gamma}, \quad \alpha\beta = C$$

el producto supuesto

$$\varphi(x) = f(x)\,F(x)$$

se convertirá en este otro:

$$C\,.\,\varphi(x) = f'(x)\,F'(x),$$

en el cual las funciones

$$f'(x) = \alpha x^m + \alpha_1 x^{m-1} + \cdots + \alpha_{m-1} x + \alpha_m$$

$$F'(x) = \beta x^n + \beta_1 x^{n-1} + \cdots + \beta_{n-1} x + \beta_n$$

tienen evidentemente coeficientes enteros. Ahora bien, segun el teorema anterior, todo factor primo p, contenido en C, debe dividir tambien á todos los coeficientes de una de las funciones $f'(x)$ ó $F'(x)$, por lo cual pueden estos factores primos suprimirse, y resultar así una nueva ecuacion

$$\varphi(x) = f''(x)\,F''(x),$$

donde las funciones $f''(x)$, $F''(x)$ son asimismo enteras, y con coeficientes enteros; y los coeficientes de las máximas potencias de su variable comun deben ser en ambas iguales á la unidad, puesto que el producto de los términos que contienen estas máximas potencias es igual al término, que en $\varphi(x)$ contiene tambien la máxima potencia de x, cuyo coeficiente es la unidad. Luego la descomposicion de $\varphi(x)$ en dos funciones enteras, pero con coeficientes fraccionarios, lleva necesariamente consigo la descomposicion de dicha funcion en funciones enteras, con coeficientes enteros: lo cual es contrario á la hipótesis, y, por consecuencia, inadmisible la descomposicion supuesta.

77.—*Composicion del primer miembro de una congruencia.*

El primer miembro de una congruencia de grado n y de módulo primo, que contenga n raices incongruentes, es igual al producto de n factores binomios cuyo primer término comun es la incógnita y cuyos segundos términos son dichas raices.

En este enunciado se supone implícitamente que el coeficiente de la más elevada potencia de la incógnita es igual á la unidad: lo cual puede siempre admitirse; puesto que, dada la congruencia general,

$$f(x) = a_0 x^n + a_1 x^{n+1} + \cdots + a_{n-1} x + a_n \equiv 0 \pmod{p},$$

en la cual no puede ser a_0 divisible por p, si hemos de considerarla como del grado n, siempre podremos encontrar (68) un número x que satisfaga á la congruencia $a_0 x \equiv 1 \pmod{p}$, multiplicar por él la general propuesta, y reducirla así á la forma particular, *ordinaria*, á que se refiere el teorema.

Hecha esta advertencia, para que se comprenda bien la exactitud del mismo, tal como está expresado, vamos á demostrar ahora que, si la congruencia de la forma general

$$f(x) \equiv 0 \pmod{p} \qquad (1)$$

contiene las n raices diferentes $\alpha, \beta, \gamma, \ldots \lambda$, será su primer miembro

$$f(x) = a_0 (x-\alpha)(x-\beta)(x-\gamma)\ldots (x-\lambda) + p\,\psi(x).$$

En efecto, siendo α raiz de la congruencia (1), si dividimos por $(x-\alpha)$ el polinomio $f(x)$, el resto r_1 de esta division será divisible por p; pues, designando por $f_1(x)$, el cociente de la misma, que será un polinomio entero con coeficientes enteros, del grado $(n-1)$, tendremos la igualdad

$$f(x) = (x-\alpha) f_1(x) + r_1 \qquad (2)$$

de donde se deduce, como es $x \equiv \alpha \pmod{p}$, $r_1 = f(\alpha) \equiv 0 \pmod{p}$.

Admitiendo que la congruencia (1) contiene otra raiz β, incongruente con α, de la última ecuacion se desprende la siguiente:

$$(\beta - \alpha) f_1(\beta) \equiv 0 \,(\text{mod. } p);$$

y de ésta, como $(\beta - \alpha)$ no puede ser divisible por p, que $f_1(\beta) \equiv 0$ (mod. p); y, por consecuencia, que β es raiz de la congruencia $f_1(x) \equiv 0 \,(\text{mod. } p)$. Dividiendo, pues, $f_1(x)$ por $(x - \beta)$, obtendremos la igualdad semejante á la anterior,

$$f_1(x) = (x - \beta) f_2(x) + r_2,$$

en la cual r_2 representa tambien un múltiplo de p, y $f_2(x)$ una funcion entera y con coeficientes enteros, del grado $(n - 2)$.

Sustituyendo ahora este valor de $f_1(x)$ en la igualdad (2), resulta esta otra:

$$f(x) = (x - \alpha)(x - \beta) f_2(x) + r_2(x - \alpha) + r_1$$

ó, como r_1 y r_2 son múltiplos de p, la siguiente:

$$f(x) = (x - \alpha)(x - \beta) f_2(x) + p\,(l\,x + m)$$

donde l y m representan números enteros.

Si todavía la congruencia (1) admitiese otra raiz γ, diferente, ó incongruente con las anteriores α y β, probaríamos, como antes, que dicha raiz γ deberia serlo de la congruencia $f_2(x) \equiv 0$, en atencion á que los factores $(\gamma - \alpha)$ y $(\gamma - \beta)$ no pueden ser divisibles por p; y obtendríamos asimismo una ecuacion de la forma

$$f(x) = (x - \alpha)(x - \beta)(x - \gamma) f_3(x) + p\,(r\,x^2 + s\,x + t).$$

en la cual r, s, t, significan números enteros.

Prosiguiendo del mismo modo, y admitido que la congruencia (1) tuviera n raices incongruentes α, β, γ..... λ, llegaríamos, por fin, evidentemente á la ecuacion,

$$f(x) = a_0 (x - \alpha)(x - \beta)(x - \gamma) \ldots\ldots (x - \lambda) + p\,\psi(x),$$

donde a_0 expresa el coeficiente de la mayor potencia de x en los po-

linomios $f(x)$, $f_1(x)$, $f_2(x)$..... cuyos grados van disminuyendo, y $\psi(x$ un polinomio cuyos coeficientes son todos números enteros.

Si la congruencia (1) la suponemos reducida á la forma ordinaria, este coeficiente a_0 no figurará en la expresion última, que podrá entónces escribirse, plenamente de acuerdo con el enunciado del teorema, de este modo:

$$f(x) = (x-\alpha)(x-\beta)(x-\gamma)..... (x-\lambda) \equiv 0 \,(\text{mod. } p).$$

78.—*Número máximo de raices de una congruencia.*

Demostrado que el polinomio de forma ordinaria $f(x)$, es equivalente al producto de los n factores binomios, $(x-\alpha)$, $(x-\beta)$,..... $(x-\lambda)$, es claro que existirán tantos modos de hacer aquel polinomio divisible por p, como haya de convertir dicho producto en múltiplo de p, y no otros diferentes. Mas, como p es primo, para que el producto

$$(x-\alpha)(x-\beta)(x-\gamma)..... (x-\lambda)$$

sea divisible por p es necesario (45) que alguno de los factores de este producto lo sea: lo cual se verifica para todos los valores α, β..... γ, congruentes con x segun p, y nada más que para estos valores; pues para otro cualquiera, μ, incongruente con ellos (mod. p), el producto

$$(\mu-\alpha)(\mu-\beta)(\mu-\gamma)..... (\mu-\lambda)$$

no podria ser divisible por p: luego

Toda congruencia de grado n no puede contener más de n raices incongruentes.

Y de aquí se deduce, que si la congruencia propuesta de grado n, $f(x) \equiv 0 \,(\text{mod. } p)$, fuese satisfecha por más de n valores congruentes con x, sería necesariamente idéntica.

79.—*Relaciones entre las raices de dos congruencias y las correspondientes de su producto.*

Si se verifica la igualdad

$$f(x) = \varphi(x)\psi(x),$$

donde las funciones $\varphi(x)$ *y* $\psi(x)$ *representan polinomios con coeficientes enteros, y la congruencia de módulo primo,*

$$f(x) \equiv 0 \,(\text{mod. } p), \qquad (1)$$

contiene tantas raices incongruentes como unidades su grado, las congruencias

$$\varphi(x) \equiv 0 \,(\text{mod. } p) \quad \text{y} \quad \psi(x) \equiv 0 \,(\text{mod. } p), \qquad (2)$$

contendrán tambien respectivamente tantas raices como unidades el mayor de los exponentes de x.

Desde luego se advierte, en efecto, que toda raiz de la congruencia (1) lo es tambien de una por lo ménos de las congruencias (2); porque de la expresion evidente

$$\varphi(\alpha)\psi(\alpha) = f(\alpha) \equiv 0 \,(\text{mod. } p),$$

se sigue que uno por lo ménos de los dos números $\varphi(\alpha)$ ó $\psi(\alpha)$, tiene que ser divisible por p. Ahora bien, si una de las dos congruencias (2) contuviese ménos raices que unidades su grado, el número de raices de la otra deberia sobrepujar á su grado; puesto que la suma de los grados de los dos polinomios $\varphi(x)$ y $\psi(x)$, es igual al grado de su producto $f(x)$; pero no es posible, segun acabamos de demostrar, que una congruencia contenga más raices que unidades su grado: luego el número de raices incongruentes de las dos congruencias, $\varphi(x) \equiv 0$ y $\psi(x) \equiv 0$ (mod. p) será igual exactamente á su grado respectivo.

Escolio. Si el módulo p de la congruencia $f(x) \equiv 0$ no fuese un número primo, el polinomio $f(x)$, igual al producto

$$(x-\alpha)(x-\beta)(x-\gamma)\ldots\ldots(x-\lambda),$$

podria ser divisible por aquél sin que lo fuera separadamente ninguno de sus factores, y entónces ocurrir el caso de que alguna de las congruencias (2) contuviese más raices que unidades su grado.

80.—*Criterio de las soluciones enteras.*

De lo dicho se desprende que existen infinidad de congruencias de grado n con n raices incongruentes; pero, dada una cualquiera de ellas, no se podrá, en general, saber por ésto solo si admitirá, ó no, soluciones en números enteros.

Existe, sin embargo, una congruencia notable, cuyas soluciones enteras se conocen siempre en valor y número, particular á primera vista, mas en realidad general y fecunda para nuestro objeto, que es la congruencia de *Fermat* (65). Refiriéndonos por de pronto al caso más general (64), esto es, al teorema de Euler,

$$x^{\varphi(k)} \equiv 1 \,(\text{mod. } k)\,,$$

podemos decir, en efecto, que esta congruencia contiene exactamente tantas raices como unidades su grado; puesto que, en primer lugar, sabemos que la satisfacen todos los números primos con k, los cuales pueden distribuirse en $\varphi(k)$ clases; y, en segundo, añadimos que sólo estos números la satisfacen; porque suponiendo que así no fuera, y que δ representase el máximo comun divisor de una raiz cualquiera x de la expresada congruencia, y de su módulo k, tenia tambien que ser δ divisor comun de los números $x^{\varphi(k)}$ y k; y por consecuencia, de los números 1 y k: lo cual es imposible no siendo $\delta = 1$.

Aplicando ahora esta doctrina al caso particular de Fermat, diremos que la congruencia

$$x^{p-1} - 1 \equiv 0 \,(\text{mod. } p)$$

contiene las $(p-1)$ raices incongruentes, segun p,

$$1\,,\quad 2\,,\quad 3\,.\,.\,.\,.\quad p-1\,,$$

y no contiene ninguna otra, diferente de éstas.

Mas, segun la proposicion (77), será

$$x^{p-1} - 1 = (x-1)(x-2)(x-3)\ldots\ldots (x-p+1) \equiv 0 \,(\text{mod. } p);$$

de donde se desprende (79) que, si la congruencia de grado n,

$$f(x) \equiv 0 \,(\text{mod. } p),$$

contiene n raices inferiores á p (como siempre se supone), deberá ser $f(x)$ divisor de $x^{p-1} - 1$: ó, con más generalidad: si la congruencia $f(x) \equiv 0$ contiene δ raices enteras, el polinomio $f(x)$ y el binomio $x^{p-1} - 1$ tendrán un divisor comun de grado δ; y, recíprocamente: si δ fuese un divisor cualquiera de $(p-1)$ tendríamos la ecuacion

$$x^{p-1} - 1 = (x^{\delta} - 1)\psi(x),$$

siendo $\psi(x)$ un polinomio con coeficientes enteros: de donde (79) se sigue que

La congruencia

$$x^{\delta} \equiv 1 \,(\text{mod. } p),$$

cuyo grado sea un divisor de $(p-1)$, *contiene siempre* δ *raices incongruentes.*

Conclúyese, por fin, que siempre podremos averiguar si una congruencia $f(x) \equiv 0$ contiene raices enteras, y cuál sea el número de estas raices, hallando el máximo comun divisor de su primer miembro $f(x)$ y del de la de Fermat, $x^{p-1} - 1$. Si este máximo comun divisor existe, y designamos su grado por δ, la congruencia $f(x) \equiv 0$ admitirá, segun hemos dicho arriba, δ raices enteras; pero, si no existe, esta congruencia no contendrá raices enteras. Así vemos, como indicamos al principio, que la congruencia de Fermat, particular á primera vista, es, no obstante, muy general en el fondo, y comprende en cierto modo á todas las demás.

81.—*Teorema de Wilson.*

Este importante teorema, demostrado por Waring é impreso por Wilson, se deduce inmediatamente de la equivalencia poco antes establecida,

$$x^{p-1} - 1 = (x-1)(x-2)(x-3)\ldots\ldots \big(x-(p-1)\big) \equiv 0 \,(\text{mod. } p).$$

Comparando los términos independientes de x en su primer miembro y en el producto desarrollado del segundo, como el número de factores negativos es par, tendremos,

$$-1 \equiv 1 \,.\, 2 \,.\, 3\ldots\ldots \,(p-1)\,(\text{mod. } p)\,;$$

ó bien

$$1 \,.\, 2 \,.\, 3\ldots\ldots \,(p-1)+1 \equiv 0\,(\text{mod. } p).$$

Este teorema en lenguaje vulgar se enuncia de este modo:

Si p es un número primo, el producto de todos los números enteros, inferiores á p, aumentado en una unidad, es un múltiplo de dicho número.

No decimos en este teorema número primo *impar*, sin embargo de que en tal supuesto lo hemos deducido, porque la congruencia de *Wilson* se verifica tambien para el único número primo, par, 2, siendo como lo son $+1$ y -1 congruentes entre sí (mod. 2).

Esta propiedad de los números primos, que demuestra el teorema de Wilson, sirve tambien para conocer si un número dado cualquiera es ó no primo. En efecto, si p es el número, siempre que se verifique la congruencia

$$1 \,.\, 2 \,.\, 3\ldots\ldots \,(p-1)+1 \equiv 0\,(\text{mod. } p)\,,$$

será primo; pues, si no lo fuera, contendria algun divisor d, diferente de la unidad y de sí mismo, que sería precisamente uno de los números 2, 3, $\ldots\ldots$ $(p-1)$, y dividiria, segun lo supuesto, á la suma

$$1 \,.\, 2 \,.\, 3\ldots\ldots \,(p-1)+1\,,$$

y evidentemente á su primer sumando; de donde resulta que el otro sumando, 1, habria de ser tambien divisible por d: lo cual es absurdo. Luego todo número primo verifica la congruencia de Wilson; y es asimismo primo todo número que la satisfaga.

La forma en cierto sentido particular de la congruencia de Fermat, fundamento conocido sobre el cual nos apoyamos para resolver las otras, nos induce á pensar que los principios expuestos en esta parte, y muy especialmente los contenidos en la última de las proposiciones referentes al número de raices de una congruencia cualquiera (de módulo primo), se hallan incluidos en una doctrina más amplia: la de las congruencias binomias, cuyo estudio debe ser nuestro punto de partida para plantear y resolver, hasta donde se pueda, el problema que principalmente constituye el objeto de nuestras actuales investigaciones.

CAPITULO III.

De las congruencias binomias.

82. — *Preliminares.*

Se llama *binomia* toda congruencia de la forma general

$$a x^n \equiv b \,(\text{mod. } k)$$

en la cual representan las letras a, b números enteros, y el exponente n un número entero y positivo.

Para resolver estas congruencias, de un modo semejante á lo que hicimos con las lineales, comenzaremos por estudiar los restos que, segun un módulo cualquiera, producen las potencias sucesivas de un número dado. Los restos de estas potencias se llaman *potenciales*, y, en particular, *cuadráticos*, *cúbicos*, etc., segun la potencia de donde proceden sea la segunda ó cuadrada, la tercera ó cúbica, etc., etc.

Si designamos por a dicho número dado y suponemos que sea primo con el módulo k, es claro que ningun término de la série de po-

tencias sucesivas de a,

$$a^0,\ a^1,\ a^2,\ a^3,\ a^4 \ldots\ldots \qquad (1)$$

será divisible por k; pero sí habrá alguno congruente con alguno de los del sistema completo de restos de k,

$$1,\ 2,\ 3,\ 4 \ldots\ldots k-1.$$

Ahora bien, como este sistema de números incongruentes (mod. k) es limitado, siempre será posible encontrar dos potencias de a, prolongando suficientemente la série anterior, que sean congruentes (mod. k): esto es, siempre podrá establecerse la congruencia

$$a^{s+u} = a^s . a^u \equiv a^s \,(\text{mod. } k);$$

de la cual se deduce (61-8.ª) esta otra:

$$a^u \equiv 1 \,(\text{mod. } k),$$

que demuestra nuevamente lo que ya sabíamos por el teorema de Euler (64): que, si a es primo con k, existe, además de la potencia a^0 siempre $\equiv 1$ (mod. k), otra potencia de a tambien congruente con la unidad respecto del módulo k. Todos los números a que satisfacen á la última congruencia se denominan *raices* n^{as} *de la unidad* (mod. k), y pueden expresarse (69-E.) por el símbolo $\sqrt[n]{1}$ (mod. k). Entre estas raices es digna de particular atencion aquella cuyo exponente sea el mínimo, exceptuando el 0. Representando por d este exponente *mínimo* para el cual se verifica la congruencia

$$a^d \equiv 1 \,(\text{mod. } k),$$

diremos en lo sucesivo que *el número* a *pertenece al exponente* d *respecto del módulo* k.

De esta definicion, y de lo dicho arriba, se infiere que las potencias sucesivas de a,

$$1,\ a^1,\ a^2,\ \ldots\ldots\ a^{d-1} \qquad (A)$$

cuyos exponentes son inferiores á d, son todas entre sí incongruentes

(mod. k); pues, si dos cualesquiera de ellas a^{s+n} y a^{s}, por ejemplo, no lo fueran, tendríamos como antes,

$$a^{s+n} \equiv a^{s} \quad \text{y} \quad a^{n} \equiv 1 \,(\text{mod. } k):$$

es decir, que no sería, contra lo supuesto, d el mínimo exponente de a. Los restos respectivos (mod. k) de las d potencias (A) constituyen lo que se llama un *período de restos* para el exponente d.

Este período de restos se repite indefinidamente, en el mismo orden, para cada d términos consecutivos de la série (1), que puede distribuirse respecto del exponente d del modo siguiente:

$$1, a^{1}, a^{2} \ldots\ldots a^{d-1} \mid a^{d}, a^{d+1} \ldots\ldots a^{2d-1} \mid a^{2d}, a^{2d+1} \ldots\ldots a^{3d-2} \mid$$

$$a^{3d}, a^{3d+1} \ldots\ldots a^{4d-1} \mid a^{4d} \ldots\ldots$$

ó bien en esta otra forma más explícita:

$$a^{d} \equiv 1, \quad a^{d+1} \equiv a, \quad a^{d+2} \equiv a^{2}, \ldots\ldots \quad a^{2d-1} \equiv a^{d-1}$$

$$a^{2d} \equiv 1, \quad a^{2d+1} \equiv a, \quad a^{2d+2} \equiv a^{2}, \ldots\ldots \quad a^{3d-1} \equiv a^{d-1}$$

$$a^{3d} \equiv 1, \quad a^{3d+1} \equiv a, \quad a^{3d+2} \equiv a^{2}, \ldots\ldots \quad a^{4d-1} \equiv a^{d-1}$$

. . . . . .

De aquí se desprende que el exponente s de una potencia cualquiera a^{s}, puede ser reemplazado por su resto mínimo respecto del exponente d á que a pertenece; pues haciendo $s = md + r$, tenemos:

$$a^{s} = a^{md+r} \equiv a^{r} \,(\text{mod. } k);$$

y además que dos potencias a^{s} y $a^{s'}$ son congruentes (mod. k) siempre que sus exponentes s y s' lo sean respecto de d: lo cual facilita muchísimo, como se observa en el cuadro anterior, la investigacion del resto (mod. k) que produce una potencia de a por grande que sea su exponente. Pero la recíproca (y ésto es lo mas importante) de la proposicion anterior es tambien cierta; porque, designando por r y r' los

restos (mod. d) de los exponentes s y s', de la congruencia entre las dos potencias de a,

$$a^s \equiv a^{s'} \text{ (mod. } k),$$

se desprende esta otra:

$$a^r \equiv a^{r'} \text{ (mod. } k) \text{ ó bien } a^{r-r'} \equiv 1 \text{ (mod. } k),$$

la cual, como r y r' son menores que d, sólo podrá verificarse cuando estos restos r y r' sean iguales; y, por consecuencia, cuando sea

$$s \equiv s' \text{ (mod. } d).$$

Ahora bien, si las dos potencias congruentes de a que se consideran son estas dos, a^0 y $a^0 = 1$, de la congruencia

$$a^s \equiv a^0 \text{ (mod. } k),$$

resultará la siguiente:

$$s \equiv 0 \text{ (mod. } d).$$

Y ésto prueba que *el exponente de toda potencia congruente con la unidad, respecto de un módulo cualquiera, es siempre divisible por el mínimo á que pertenece la base de dicha potencia respecto del mismo módulo;* ó, en otros términos, que *toda raiz* n^a *de la unidad pertenece á un exponente que es un divisor de* n. Así, de la congruencia de Euler ya conocida

$$a^{\varphi(k)} \equiv 1 \text{ (mod. } k),$$

se deduce que el exponente d á que el número a pertenece, respecto de k, es siempre divisor de $\varphi(k)$.

83.—*De las raices primitivas.*

En general llaman los autores que tratan de la materia *raices primitivas* á todos los valores de x que satisfacen á la congruencia $x^n \equiv 1$; pero no á otra semejante de grado inferior. Nosotros, sin embargo, conformes en parte con alguno de aquellos (*), daremos á tales valores el

(*) Poinsot, otra ya citada.

nombre genérico de *raices propias* de la congruencia $x^n \equiv 1$; y el especial de *primitivas* á las propias de la congruencia particular $x^{\varphi(k)} \equiv 1$ (mod. k), ó bien á los números pertenecientes al exponente $\varphi(k)$ respecto del módulo k. Así, un número a primo con k será raiz primitiva de esta última congruencia, cuando ninguna de sus potencias de grado inferior á $\varphi(k)$ sea $\equiv 1$ (mod. k); y tambien podremos decir que las raices n^{as} de la unidad (mod. k) pertenecientes al exponente d coinciden con las raices propias de la congruencia $x^d \equiv 1$ (mod. k).

Apoyándonos en la misma congruencia de Euler es fácil determinar previamente en qué casos, segun la naturaleza del módulo k, es posible que existan raices primitivas para dicho módulo.

Supongamos, y es el más general, que

$$k = p^{\pi}\, r^{\rho}\, s^{\sigma};$$

en cuya forma representan $p, r, s, \ldots$ números primos diferentes. Entónces (55)

$$\varphi(k) = \varphi(p^{\pi})\varphi(r^{\rho})\varphi(s^{\sigma}) \ldots = p^{\pi-1}(p-1) \cdot r^{\rho-1}(r-1) \cdot s^{\sigma-1}(s-1) \ldots$$

Si a es primo con k, y, por lo tanto, primo con cada uno de los factores de k, conforme con la congruencia de Euler, estableceremos las siguientes:

$$a^{\varphi(p^{\pi})} \equiv 1 \text{ (mod. } p^{\pi})$$

$$a^{\varphi(r^{\rho})} \equiv 1 \text{ (mod. } r^{\rho})$$

$$a^{\varphi(s^{\sigma})} \equiv 1 \text{ (mod. } s^{\sigma})$$

. . . . . .

Designando ahora por h el producto $\varphi(k)$ de los exponentes de estas congruencias, $\varphi(p^{\pi})$, $\varphi(r^{\rho})$, $\varphi(s^{\sigma}) \ldots$, resultará (66) finalmente esta otra:

$$a^h \equiv 1 \text{ (mod. } k).$$

Pero $\varphi(p^{\pi})$, $\varphi(r^{\rho})$, $\varphi(s^{\sigma}) \ldots$, son números pares, excepto en el

caso (56) de que respectivamente sean $p=2$, $\pi=1$; $r=2$, $\rho=1$; etc.: luego siempre que k contenga más de un factor primo impar, ó bien un solo factor de esta clase y el factor 2 elevado á una potencia superior á la primera, dos por lo ménos de los números $\varphi(p^{\pi})$, $\varphi(r^{\rho})$, $\varphi(s^{\sigma})$....., tendrán un factor comun, y, de consiguiente, su mínimo comun múltiplo (44) será menor que su producto h: es decir, que existe entónces un exponente de a inferior á $\varphi(k)$ que verifica la congruencia de Euler: lo cual prueba que a no es raiz primitiva de k.

Examinemos ahora el caso en que el módulo

$$k=2^{\lambda},$$

no contenga ningun factor primo impar. Todo número impar a, primo con 2 naturalmente, podemos expresarlo bajo la forma

$$a=\pm 1+2^{2}n;$$

la cual, elevada sucesivamente al cuadrado, produce las siguientes:

$$\begin{aligned}
a^{2}&=1+2^{3}n_{1}\\
a^{2^{2}}&=1+2^{4}n_{2}\\
a^{2^{3}}&=1+2^{5}n_{3}\\
&\cdots\cdots\cdots\cdots\\
a^{2^{\lambda-2}}&=1+2^{\lambda}n_{\lambda-2}
\end{aligned}$$

Esta última igualdad, como $\varphi(2^{\lambda})=2^{\lambda-1}$, puede escribirse así:

$$a^{\frac{1}{2}\varphi(2^{\lambda})}\equiv 1\ (\text{mod. } 2^{\lambda}):$$

congruencia que se verifica siempre que sea $\lambda>2$; y ésto prueba que a no es entónces raiz primitiva de 2^{λ}.

Pero, si fuese $\lambda\leqq 2$, esto es, $\lambda=0,\ 1,\ 2;\ 2^{\lambda}$, por consecuencia, igual á $1,\ 2,\ 4$ y $\varphi(2^{\lambda})=1,\ 1,\ 2$, la congruencia anterior nos conduciria á un absurdo, y en cambio se verificaria para los tres casos expresados esta otra:

$$a^{\varphi(2^\lambda)} \equiv 1 \pmod{2^\lambda};$$

la cual manifiesta que a entónces puede ser raiz primitiva del módulo 2^λ. Y, en efecto, todo número impar es raiz primitiva de los módulos 2^0 y 2^1; y el número 3 ó -1 satisface tambien á la congruencia

$$3^{\varphi(4)} \equiv 1 \pmod{4}$$

evidentemente, y es, por lo tanto, raiz primitiva de 2^2.

Ahora bien, de la congruencia $a \equiv a' \pmod{k}$ se deduce $a^s \equiv a'^s \pmod{k}$, y de aquí que dos números cóngruos pertenecen al mismo exponente; y, por consecuencia, que los únicos números que debemos elevar á las potencias sucesivas para hallar sus restos, y ver por ellos los exponentes á que pertenecen, segun un módulo cualquiera, son los que forman el sistema completo de números incongruentes para dicho módulo. Uno de estos números incongruentes a, respecto de k, hemos tomado como base de los anteriores razonamientos; y, puesto que lo mismo que del número a puede decirse de todos los incongruentes (mod. k), resulta, por fin, que sólo pueden existir raices primitivas:

1.° *Cuando el módulo k sea un número primo impar.*

2.° *Cuando el módulo k sea una potencia superior á la primera de un número primo impar ó el duplo de tal potencia.*

3.° *Cuando el módulo k sea igual á* 1, 2 *ó* 4.

Estudiaremos en particular, y con la minuciosidad que la importancia de cada uno de ellos exija, los tres casos enumerados.

84.—*De los números pertenecientes á un exponente dado respecto de un módulo primo impar.*

El teorema de Fermat,

$$a^{p-1} \equiv 1 \pmod{p},$$

enseña, conforme á los principios generales explicados en el párrafo anterior, que el exponente d á que pertenece el número a (no divisible por p) respecto del módulo p, debe ser siempre un divisor de $\varphi(p) = p - 1$.

Admitido que d sea efectivamente un divisor de $p - 1$, ¿existirán

siempre números a pertenecientes á dicho exponente d?; y, si en realidad existen, ¿podremos saber cúales y cuántos son en suma? Demostrado ya que es posible, en las actuales condiciones del módulo, la existencia de números pertenecientes al exponente $p-1$, supongamos en general que un número por lo ménos, a, pertenece en efecto á un divisor cualquiera d de $p-1$. Entónces los d números

$$a,\quad a^2,\quad a^3,\ldots..\ a^{d-1},\quad a^d\equiv 1,$$

ó bien, escribiendo primeramente el último,

$$1,\quad a,\quad a^2,\ldots.,\ a^{d-1}, \qquad (A)$$

serán, segun ya probamos (82), incongruentes (mod. p); y como de la congruencia previamente admitida,

$$a^d\equiv 1\ (\text{mod. } p),$$

se desprende esta otra,

$$\left(a^d\right)^r=\left(a^r\right)^d\equiv 1\ (\text{mod. } p),$$

es claro que los d números (A) son raices de la congruencia de grado d

$$x^d\equiv 1\ (\text{mod. } p).$$

Resulta, pues, que los números buscados, pertenecientes al exponente d, deben satisfacer á esta congruencia; y como sus d únicas raices, verdaderamente distintas, son los números incongruentes de la série (A), entre estos se hallarán los que buscamos.

Tomemos ahora uno cualquiera de ellos; el a^r, por ejemplo; y propongámonos averiguar cuál es el exponente, h, á que pertenece. Por definicion tenemos que:

$$(a^r)^h=a^{rh}\equiv 1\ (\text{mod. } p).$$

Y como a, por definicion ó hipótesis tambien, pertenece al exponente d, resulta que rh debe ser divisible por d. Si representamos ahora por δ el máximo comun divisor de r y d, podremos escribir estas igualdades:

$$r=r'\delta \quad \text{y} \quad d=d'\delta;$$

de las cuales se desprende que $rh=r'\delta h$, debe ser divisible por $d=d'\delta$; ó h por d'. A esta última condicion se satisfará de la manera

mas sencilla suponiendo que $h = d'$: y, como para este valor d' es efectivamente

$$(a^r)^{d'} = (a^d)^{r'} \equiv 1 \,(\text{mod. } p),$$

conclúyese que al exponente d' corresponden ó pertenecen todos los números de la série (A) cuyos exponentes tienen con d el máximo comun divisor $\delta = d : d'$. Y por lo tanto: que al exponente d pertenecen todos aquellos números, $\varphi(d)$, en totalidad, cuyos exponentes son primos con d; porque entónces $\delta = 1$ y forzosamente $d' = d$.

Hasta aquí hemos demostrado que, *si existe uno*, existen precisamente $\varphi(d)$ números pertenecientes al exponente d; pero nos queda la duda todavía de si no existirá ninguno.

Para desvanecerla distribuyamos los $(p-1)$ números incongruentes segun p,

$$1,\quad 2,\quad 3, \ldots\ldots (p-1),$$

en grupos, cada uno de los cuales contenga exclusivamente los que pertenezcan á uno solo de los divisores d de $(p-1)$. Si representamos por $\psi(d)$ el conjunto de los individuos del sistema de restos de p que pertenecen á un divisor cualquiera d, de $(p-1)$, como ninguno de estos $(p-1)$ restos ó números incongruentes (mod. p) puede figurar sino en un solo de los grupos $\psi(d)$, es claro que

$$\Sigma \psi(d) = p - 1,$$

siempre que el signo sumatorio se refiera á todos los divisores d de $(p-1)$: mas tambien (57)

$$\Sigma \varphi(d) = p - 1.$$

y, por consecuencia:

$$\Sigma \psi(d) = \Sigma \varphi(d);$$

de cuya igualdad se deduce que nunca podrá ser $\psi(d) = 0$ sino $= \varphi(d)$; porque cada sumando $\psi(d)$ de su primer miembro todo lo más que puede valer, segun lo demostrado antes, es tanto como el correspondiente $\varphi(d)$ del segundo; y, de consiguiente, si aconteciere que una ó más veces fuese $\psi(d) = 0$, la suma $\Sigma \psi(d)$ valdria ménos que $\Sigma \varphi(d)$: lo cual es inadmisible siendo ambas sumas iguales. Luego

El conjunto de los números incongruentes (mod. p) que pertenecen á un divisor determinado d de $\varphi(p) = p - 1$, es siempre $\varphi(d)$.

85.—*De las raices primitivas de un módulo primo impar.*

Habiéndonos referido en la última demostracion á un divisor cualquiera de $\varphi(p)$, y no en particular á ninguno determinado, muy bien podríamos aplicar las precedentes conclusiones á los números pertenecientes al mismo $\varphi(p) = p - 1$, esto es, á las raices primitivas de p, y sentar desde luego que:

Existen siempre $\varphi(\varphi(p)) = \varphi(p-1)$ *raices primitivas* g *del número* p, *cuyas potencias sucesivas*

$$1,\ g,\ g^2,\ \ldots\ g^{p-2}, \qquad (G)$$

divididas por p, *producen el sistema completo de restos* (*mod.* p).

Y además que:

Entre las potencias (G) *pertenecerán á un divisor,* d, *de* $(p-1)$, *aquellas cuyos exponentes tengan comun con* $(p-1)$ *el máximo divisor* $\delta = (p-1) : d$.

Pero, como indispensable para lo sucesivo, demostraremos estos principios por otro método, tambien más directo, que se funda en el siguiente

Teorema. Si establecemos la igualdad

$$\varphi(p) = p - 1 = a^{\alpha}\, b^{\beta}\, c^{\gamma} \ldots\ldots$$

(*siendo* a, b, c..... *números primos diferentes*), *y* A, B, C..... *representan números que pertenecen á los exponentes* a^{α}, b^{β}, c^{γ}..... *respectivamente, el producto* $ABC\ldots\ldots = P$ *pertenecerá al producto*

$$a^{\alpha}\, b^{\beta}\, c^{\gamma} \ldots\ldots = \varphi(p),$$

ó será raiz primitiva del número primo p.

Para demostrarlo observaremos ante todo que el producto $ABC\ldots\ldots$ es raiz de la congruencia

$$x^{p-1} \equiv 1 \pmod{p};$$

puesto que $p-1$ es divisible por los números a^{α}, b^{β}, c^{γ}....; y, como los números A, B, C..... pertenecen, por hipótesis, á los exponentes a^{α}, b^{β}, c^{γ}....., resulta que A^{p-1}, B^{p-1}, C^{p-1}...., será, cada uno, congruente con la unidad (mod. p); y, por consecuencia, su producto $(ABC.....)^{p-1}$ lo será tambien. De modo que, si probásemos que el exponente $p-1$ es el mínimo para el cual dicho producto da el resto 1 (mod. p), la demostracion estaria terminada. Supongamos, pues, que así no suceda; sino que, por el contrario, sea d, divisor de $p-1$, distinto de este número, el exponente á que tal producto pertenezca. El divisor d contendrá, por lo tanto, ménos veces que $p-1$ alguno de los factores, a, por ejemplo, de este número; y podremos en este supuesto establecer la congruencia:

$$P^{d'} = P^{a^{\alpha'} b^{\beta} c^{\gamma}.....} \equiv 1 \text{ (mod. } p);$$

en la cual será $\alpha' < \alpha$; y tambien, refiriéndose al número A, esta otra:

$$A^{a^{\alpha'} b^{\beta} c^{\gamma}} \equiv 1 \text{ (mod. } p).$$

Mas, segun la hipótesis del teorema, es

$$A^{a^{\alpha}} \equiv 1 \text{ (mod. } p);$$

y, como siempre es posible (70) hallar dos números enteros, x é y, que verifiquen la igualdad

$$x \cdot a^{\alpha} + y \cdot a^{\alpha'} b^{\beta} c^{\gamma} \ldots \ldots = a^{\alpha'},$$

por ser $a^{\alpha'}$ el máximo comun divisor de a^{α} y $a^{\alpha'} b^{\beta} c^{\gamma}$.....,
de las dos últimas congruencias resultaría finalmente:

$$A^{a^{\alpha'}} \equiv 1 \text{ (mod. } p),$$

en contradiccion con lo admitido de ser a^{α} el exponente á que pertenece el número A. Luego no puede suponerse que el producto $ABC.... = P$ pertenezca á un exponente menor que $p-1$: lo cual prueba que tal producto es raiz primitiva de p.

Pero este resultado, como el que obtuvimos poco antes (84), se funda tambien en la hipótesis de que existan los números A, B, C..... pertenecientes á los divisores a^{α}, b^{β}, c^{γ}...., de $p-1$; por manera que, si el género de demostracion que ahora empleamos se ha de diferenciar del anterior, es necesario que lo admitido allí préviamente como hipotético, lo establezcamos aquí desde luego, directamente, como de realidad incontrovertible.

Comenzaremos por recordar, para esto, que si a representa un divisor de $p-1$, entre los términos del sistema completo de restos (mod. p),

$$1,\ 2,\ 3,\ .....\ (p-1),$$

habrá $(p-1):a$ solamente (78) que satisfarán á la congruencia de módulo primo

$$x^{\frac{p-1}{a}} \equiv 1 \pmod{p}; \qquad (1)$$

y no la satisfarán los restantes hasta el completo de $p-1$. Esta clase de términos existirá siempre que el divisor elegido, a, de $p-1$, no sea el mismo $p-1$; pues en este caso la última congruencia se reduciría á la de primer grado

$$x \equiv 1 \pmod{p},$$

que tiene por única raiz 1. Si designamos por g uno de ellos, esto es, uno de los que no satisfagan á la congruencia (1), su potencia $(p-1):a$, y tambien su potencia $(p-1):a^{\alpha}$, será incongruente con la unidad: así que podremos establecer la nueva congruencia

$$g^{\frac{p-1}{a^{\alpha}}} \equiv h \pmod{p}; \qquad (2)$$

de la cual, elevándola á la potencia a^{α} y teniendo presente el teorema de Fermat, se desprende esta otra:

$$h^{a^{\alpha}} \equiv 1 \text{ (mod. } p\text{)}:$$

que manifiesta ser el resto h, de la potencia $(p-1):a^{\alpha}$ de g, elevado á la potencia a^{α}, congruente con la unidad. Si demostramos ahora que a^{α} es el mínimo exponente que hace la potencia $h^{a^{\alpha}}$ congruente con la unidad, habremos conseguido lo que pretendíamos: hallar un número h perteneciente al exponente a^{α}. Pero la demostracion de ésto es muy sencilla. En efecto: de la congruencia (2) se deduce que la potencia $a^{\alpha-1}$ de h, congruente con la $(p-1):a$ de g, es incongruente con la unidad; y con mayor razon lo serán las potencias $a^{\alpha-2}$, $a^{\alpha-3}$, ... etc., de h; mas el exponente á que h pertenezca debe ser divisor de a^{α}, y esta potencia, por ser a número primo, no contiene factores diferentes de su base; luego será ella misma el exponente á que h pertenece. Tenemos, por consecuencia, que si g representa uno de los restos de p que no satisfacen á la congruencia (1), el resto h (mod. p) de la potencia $(p-1):a^{\alpha}$ de g, es efectivamente un número que pertenece al exponente a^{α}: cosa semejante puede afirmarse respecto de todos los otros divisores, b^{β}, c^{γ}..... de $p-1$; y concluirse, por fin, que existen siempre números pertenecientes (mod. p) á los divisores de $p-1$, y por lo tanto, raices primitivas de p.

Demostrado por completo el teorema enunciado, es evidente que todos los productos distintos, ó combinaciones posibles de los números A, B, C..... que pertenezcan á los exponentes a^{α}, b^{β}, c^{γ}, ... primos entre sí, serán precisamente los números que pertenecen al producto de estos, $p-1$, esto es: las raices primitivas de p; y el número de todas aquellas combinaciones, ó productos diferentes, el de estas raices primitivas. Ahora bien, sabido ya ciertamente que existen siempre números A, B, C..... pertenecientes á los exponentes a^{α}, b^{β}, c^{γ}....., probado tenemos (84) que al exponente a^{α} pertenecerán

$\varphi(a^\alpha)$ números A; al b^β, $\varphi(b^\beta)$ números B; al c^γ, $\varphi(c^\gamma)$ números C..... etc.; el número total de las combinaciones de todas clases que pueden efectuarse con los $\varphi(a^\alpha)$ números A, los $\varphi(b^\beta)$ números B, los $\varphi(c^\gamma)$ números C....., etc., es: $\varphi(a^\alpha)\ \varphi(b^\beta)\ \varphi(c^\gamma)$... ; y, como este producto es igual á $\varphi(a^\alpha . b^\beta . c^\gamma .....) = \varphi(p-1)$, este será tambien el número de las raices primitivas de p.

86.—*Método para hallar las raices primitivas de un número primo impar.*

Del procedimiento empleado en la demostracion anterior se desprende una regla sencilla para calcular los números pertenecientes á los divisores de $p-1$, y determinar, en consecuencia, las raices primitivas de p, que aplicaremos desde luego á un ejemplo.

Sea el módulo

$$p = 73;\quad p-1 = 72 = 2^3 . 3^2;$$

y, por lo tanto:

$$a = 2,\quad b = 3,\quad \frac{p-1}{a} = 36,\quad \frac{p-1}{b} = 24;\quad \frac{p-1}{a^\alpha} = 9;\quad \frac{p-1}{b^\beta} = 8.$$

Los primeros números del sistema completo de restos (mod. 73), cuyas potencias 36 y 24 son incongruentes con la unidad, son 5 y 2; puesto que efectivamente tenemos:

$$\left.\begin{array}{l} 5^3 \equiv -21,\ 5^6 \equiv 3,\ 5^{12} \equiv\ \ 9,\ 5^{24} \equiv 8,\ 5^{36} \equiv 8 . 9 \equiv -1 \\ 2^3 \equiv 8,\ 2^6 \equiv -9,\ 2^{12} \equiv 8,\ 2^{24} \equiv 8^2\ \equiv -9 \end{array}\right\} (\text{mod. } 73).$$

Los divisores de $p-1 = 72$ son los siguientes:

$$1,\ 2,\ 3,\ 4,\ 6,\ 8,\ 9,\ 12,\ 18,\ 24,\ 36,\ 72.$$

Al divisor 1 pertenece solamente el número 1; al divisor $2 = a$, el

número $5^{36} \equiv -1$, ó bien el 72; al divisor $3 = b$, desde luego el número $2^{24} \equiv -9$; y, como los números inferiores y primos con 3 son 1 y 2, los restos de las potencias $(-9)^1$ y $(-9)^2$, esto es, 64 y 8, pertenecerán al exponente 3..... etc. El resto de la potencia 5^9 es

$$-21 . 3 = -63 \equiv 10 \text{ (mod. 73)};$$

el de la potencia 2^8 es $4 . -9 = -36 \equiv 37$; de lo cual se deduce que 10 pertenece al exponente $8 = a^\alpha = 2^3$; y 37 pertenece al exponente $9 = b^\beta = 3^2$; y, por consecuencia, el producto

$$10 . 37 = 370 \equiv 5 \text{ (mod. 73)}$$

pertenece al exponente $72 = p - 1$, ó bien, 5 es raiz primitiva del módulo 73. Hallada la raiz primitiva 5, todas las demás serán los restos (mod. 73) de las potencias de 5 suyos exponentes sean los números primos con $72 = p - 1$, é inferiores á este número.

87.—*Otro método.*

El que acabamos de explicar es muy pesado en la práctica, sobre todo cuando se trate de un módulo ya un poco considerable; el actual (*), por tanteo, como el anterior, hasta cierto punto, tiene la ventaja de ser más expedito.

Elíjase á voluntad un número a, primo con el módulo p (que la mayor parte de las veces convendrá que sea el mínimo, 2), y calcúlese su período, esto es, los restos de sus potencias sucesivas hasta llegar, prescindiendo de la potencia cero, á una $\equiv 1$ (mod. p): si el exponente de esta potencia fuese $p - 1$, claro es que a sería raiz primitiva de p; mas demos por seguro que así no suceda, sino que, por el contrario,

(*) Gauss, D. A. §. 73.

pertenezca el número a al exponente $m < p-1$; y ensayemos otro número b, no contenido en el período del precedente a, el cual supondremos que pertenece al exponente n, menor tambien que $p-1$; puesto que, si fuera $n = p-1$, ya sería b raiz primitiva. Como el número b no figura entre los términos del período de a, es evidente que el exponente n no puede ser igual á m, ni factor del mismo; pero, si fuese n múltiplo de m, ya pertenecería el número b á un exponente mayor que el del número a, y más próximo, por consecuencia, del máximo, $p-1$, que buscamos. Ahora bien, este número que pertenece á un exponente mayor, y más próximo á $p-1$, por cuyo medio va progresivamente avanzando la resolucion del problema propuesto, podemos siempre determinarlo, aunque no sea n múltiplo de m. En efecto: designemos por μ el mínimo comun múltiplo de los números m y n; y descompongámoslo (43) en dos factores primos entre sí, m' y n', divisor el uno de m, y de n el otro: y entónces, de las congruencias hipotéticas,

$$a^{m:m'} \equiv A \quad \text{y} \quad b^{n:n'} \equiv B \,(\text{mod. } p);$$

se desprenden estas otras:

$$a^{m} \equiv A^{m'} \equiv 1 \quad \text{y} \quad b^{n} \equiv B^{n'} \equiv 1 \,(\text{mod. } p);$$

y, de aquí, como m' y n' son primos entre sí, la siguiente:

$$(A\,B)^{m'n'} = (A\,B)^{\mu} \equiv 1 \,(\text{mod. } p),$$

que determina el número que deseábamos.

Calculando de este modo números que sucesivamente vayan perteneciendo á exponentes mayores, por precision habremos de llegar á uno que pertenezca al máximo, $p-1$, y este será el que se busca.

Ejemplo. Sea $p = 73$. Tomemos el menor número primo con 73, que es 2, y formemos su período:

$$2,\ 4,\ 8,\ 16,\ 32,\ 64,\ 55,\ 37,\ 1,$$

el cual, como tiene 9 términos, prueba que 2 pertenece al exponente 9.

Calculando ahora el período del número 3 que no figura entre los términos del período de 2, tendremos los 12 términos:

3, 9, 27, 8, 24, 72, 70, 64, 46, 65, 49, 1.

cuyo número indica que 3 pertenece (mod. 73) al exponente 12. El mínimo comun múltiplo de los exponentes 9 y 12 es 36 = al producto de dos números primos entre sí, 9 y 4, que dividen respectivamente á 9 y 12, siendo los cocientes 1 y 3: de modo que $2^1 \times 3^3 = 54$, pertenecerá al exponente 36. Formemos ahora el período de 54, y obtendremos los 36 términos:

54, 69, 3, 16, 61, 9, 48, 37, 27, 71, 38, 8, 67, 41, 24, 55, 50, 72,

19, 4, 70, 57, 12, 64, 25, 36, 46, 2, 35, 65, 6, 32, 49, 18, 23, 1:

cuyo cálculo es sencillo, si tenemos en cuenta que un término cualquiera es igual al resto (mod. 73) del producto por 3 del que le precede en 3 lugares, por ser 3 el resto (mod. 73) del cubo de 54.

Fijándonos en el número 5, vemos que no está comprendido entre los 36 últimos; pero lo está su cuadrado 25 ocupando el lugar 25: lo cual manifiesta que 25 es resto de la potencia 25 del mismo 54; y, como 25 y 72 son primos entre sí, que 25 pertenece al exponente 36; y, por consecuencia, 5 al exponente $36 \times 2 = 72$, es decir, que 5 es la raiz que buscábamos. En este ejemplo hemos visto que ciertas circunstancias han contribuido á simplificar todavía más el procedimiento general antes explicado.

Hallada una raiz primitiva, g, de un número primo p, de la série de potencias de esta raiz primitiva, se pueden tambien deducir fácilmente los números pertenecientes á los divisores, d, de $p - 1$, multiplicando los números inferiores, y primos con d, por $\delta = (p - 1) : d$; y calculando despues los restos de las potencias de g cuyos exponentes sean estos productos.

Un ejemplo completo, mejor que explicaciones minuciosas, pondrá en claro éste y los demás particulares que sobre la misma materia hemos indicado anteriormente.

Ejemplo. Sea el número ó módulo propuesto, $p = 13$; elevemos á

las potencias sucesivas 1.ª, 2.ª..... 12.ª, todos los individuos del sistema completo de restos (mod. 13), 1, 2, 3..... 12; y así formaremos el cuadro siguiente:

Exponentes.	*Restos de las potencias de los números incongruentes* (mod. 13).											
1	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
2	1	4	9	3	12	10	10	12	3	9	4	1
3	1	8	1	12	8	8	5	5	1	12	5	12
4	1	3	3	9	1	9	9	1	9	3	3	1
5	1	6	9	10	5	2	11	8	3	4	7	12
6	1	12	1	1	12	12	12	12	1	1	12	1
7	1	11	3	4	8	7	6	5	9	10	2	12
8	1	9	9	3	1	3	3	1	3	9	9	1
9	1	5	1	12	5	5	8	8	1	12	8	12
10	1	10	3	9	12	4	4	12	9	3	10	1
11	1	7	9	10	8	11	2	5	3	4	6	12
12	1	1	1	1	1	1	1	1	1	1	1	1

Los divisores de $p - 1 = 12$ son 1, 2, 3, 4, 6, 12; y estos son los exponentes á que todos los números del sistema completo de restos (mod. 13) pertenecen. Al divisor 1 pertenece el *único* número 1; al exponente 2 pertenece otro *solo* número: el 12; al exponente 3 los *dos* números 3 y 9; al 4 tambien *dos* números: 5 y 8; al 6 otros *dos:* 4 y 10; y, últimamente, al divisor 12 los *cuatro* números, 2, 6, 7, 11, que son las raices primitivas de 13. Estos resultados patentizan que á cada divisor, d, de 12, pertenecen $\varphi(d)$ números de entre los incongruentes (mod. 13); y además, que:

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = \Sigma\varphi(d) = 12.$$

Si al exponente 6 pertenece el número 4, las potencias sucesivas de 4 hasta la 6.ª, ó los restos de estas potencias, formarán el período de este número, y entre estos restos, los de potencias cuyos exponentes sean primos con 6, pertenecerán asimismo al exponente 6. En efecto:

Potencias: $4,\ 4^2,\ 4^3,\ 4^4,\ 4^5,\ 4^6$

Restos (mod. 13): 4, 3, 12, 9, 10, 1;

donde se ve que $10 \equiv 4^5 \pmod{13}$ pertenece al exponente 6 primo con el exponente 5 de la potencia 4^5. Si formamos el período de una raiz primitiva, 2, por ejemplo, tendremos:

Potencias: $2,\ 2^2,\ 2^3,\ 2^4,\ 2^5,\ 2^6,\ 2^7,\ 2^8,\ 2^9,\ 2^{10},\ 2^{11},\ 2^{12},$

Restos: 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1.

El período de una raiz primitiva comprende, segun vemos, todos los términos del sistema completo de números incongruentes (mod. 13); y conocido este período de la raiz primitiva 2, todas las demás se calculan facilmente. Así; los números 2, 6, 7 y 11, que son restos de potencias cuyos exponentes son primos con 12, son raices, y todas las raices primitivas, de 13. Al divisor 1 de 12 pertenece el 2^{12}, cuyo exponente tiene comun con 12 : 1 el máximo divisor 12; al divisor 2 pertenece el número 12 ó 2^6, cuyo exponente 6 tiene comun con 12 el máximo divisor $6 = 12 : 2$; al divisor 4 pertenecen los números $8 \equiv 2^3$ y $5 \equiv 2^9$, cuyos exponentes 3 y 9 tienen comun con 12 el máximo divisor $12 : 4 = 3$; etc. Con los divisores d de 12, sus complementarios δ, y los números inferiores y primos con cada uno de los primeros, formamos el cuadro siguiente:

δ	d	*Primos con d.*	*Productos por δ' de los primos con d.*	*Potencias correspondientes de 2.*
1	12	1, 5, 7, 11	1, 5, 7, 11	$2,\ 2^5,\ 2^7,\ 2^{11}$
2	6	1, 5	2, 10	$2^2,\ 2^{10}$
3	4	1, 3	3, 9	$2^3,\ 2^9$
4	3	1, 2	4, 8	$2^4,\ 2^8$
6	2	1	6,	2^6
12	1	1	12,	2^{12}

Los productos 1, 5, 7, 11 son los exponentes de las potencias de 2, cuyos restos (mod. 13) son los números que pertenecen al exponente 12; los restos de las potencias 2^2, 2^{10}, que son 4 y 10, son los números que pertenecen al exponente 6; etc.

Para terminar este asunto daremos á continuacion una lista de los números primos impares, inferiores á 100, con sus mínimas raices primitivas correspondientes.

Números =	3,	5,	7,	11,	13,	17,	19,	23,	29,	31,	37,	41
Raices =	2,	2,	3,	2,	2,	3,	2,	5,	2,	3,	2,	6

Números =	43,	47,	53,	59,	61,	67,	71,	73,	79,	83,	89,	97
Raices =	3,	5,	2,	2,	2,	2,	7,	5,	3,	2,	3,	5.

Complemento de la doctrina general anterior.

De los principios antes demostrados se desprenden numerosas consecuencias, entre las cuales merecen fijar nuestra atencion las que seguidamente se expresan:

1.ª *El número de los números que pertenecen á un exponente cualquiera es siempre par, exceptuando los dos únicos casos en que tal exponente sea* 1 *ó* 2. Pues entónces $\varphi(1)$ y $\varphi(2)$ son la unidad.

2.ª Dos números cuyo producto sea cóngruo con la unidad (mod. p) se llaman *socios* segun p.

Todos los números que pertenecen al mismo exponente (mod. p), *mayor que* 2, *son sócios dos á dos, segun* p. En efecto: perteneciendo el número a al exponente d (mod. p), si r es primo con d, y menor que este número, pertenecerá a^r al exponente d (84); y, como $d-r$ es tambien primo con d (55), pertenecerá asimismo a^{d-r} al exponente d; pero

$$a^r \cdot a^{d-r} = a^d \equiv 1 \pmod{p}:$$

luego a^r y a^{d-r} son sócios. Falta, sin embargo, demostrar que a^{d-r} es el único socio de a^r. Para esto admitamos, por un momento, que

exista un exponente r' diferente de $d-r$, menor que d y primo con d, de modo que se verifique la congruencia

$$a^{r}.a^{r'}=a^{r+r'}\equiv 1\,(\text{mod. } p);$$

esto pide que $r+r'$ sea un múltiplo de d; pero r y r' son, por hipótesis, ambos menores que d; y, por consecuencia, $r+r'$ menor que $2d$: luego no puede admitirse la suposicion de que a^{r} tenga un socio distinto de a^{d-r}.

Los exponentes de los números socios son complementarios respecto del exponente á que éstos pertenecen.

De aquí se sigue que:

3.ª *El producto de todos los números que pertenecen al mismo exponente* (mayor que 2) *es cóngruo con la unidad.*

4.ª *Los períodos de todos los números que pertenecen al mismo exponente según un módulo dado, constan de los mismos términos, aunque en diferente órden.* Pues, si a pertenece al exponente d, y r es primo con d, pertenecerá tambien (84) a^{r} al exponente d. Los restos de la série de potencias (82)

$$a.\ a^{2}.\ a^{3},\ a^{4},\ldots\ldots\ a^{d}.$$

se reproducen periódicamente de d en d; y, como en esta série de potencias, prolongada suficientemente, se encontrará cualquiera de a^{r}, por ejemplo, a^{nr}, resulta que esta otra série

$$a^{r},\ a^{2r},\ a^{3r}\ldots\ldots\ a^{dr},$$

producirá los mismos restos, prescindiendo del órden, que la anterior (63). Asi el período del número 2 que pertenece al exponente 9 (mod. 73), es:

$$2,\ 4,\ 8,\ 16,\ 32,\ -9,\ -18,\ -36,\ 1;$$

y de los mismos términos, aunque en órden diferente, constan los períodos de los números 37, 4 y 55, 16 y 32, que asimismo pertenecen al exponente 9. Además son socios: 2 y 37, 4 y 55, 16 y 32.

5.ª *Si en un período de restos correspondiente á un número cualquiera* (diferente de 0) *prescindimos del último término* 1, *los equidistantes de los extremos son socios.* Pues, si establecemos que, en el caso de que sea impar el número de términos que queden en el período, suprimido el último, el único término del medio entónces existente sea socio de sí mismo, podemos, en general, afirmar que las formas de dos cualesquiera de estos términos equidistantes de los extremos del período (restringido) son a^s y a^{d-s} cuyo producto es: $a^s \cdot a^{d-s} = a^d \equiv 1 \pmod{p}$ (2.ª).

Con mucha facilidad se demostraria despues de lo dicho que:

6.ª *Los períodos* (fuera de su último término) *de dos números socios, constan de los mismos términos, pero en órden inverso.*

Y tambien que:

7.ª *Si se suprime un número cualquiera de términos sucesivos de un período cualquiera, los productos de cada dos números equidistantes de los extremos en el período parcial restante, son entre sí congruentes segun el módulo á que dicho período se refiera.*

8.ª *Entre los términos del período de un número* a, *perteneciente á un exponente* d (mod. p), *no se hallará nunca el término* -1, *cuando* d *sea impar; mas, si* d *es par, se hallará una sola vez el término* -1, *y este resto corresponderá precisamente á la potencia* $\frac{d}{2}$ *de* a, *ó en general á la potencia* $n\,d + \frac{d}{2}$. En efecto: si d es impar, cualquier número par, $2r$, dejará un resto $r' < d$, al ser dividido por d; y de consiguiente, podemos darle la forma $2r = n\,d + r'$. Admitiendo ahora que se verifique, contra la conclusion primera, la congruencia

$$a^{r'} \equiv -1, \text{ y, por lo tanto, } a^{2r'} \equiv 1 \pmod{p};$$

y, poniendo por $2r$ su valor, se obtienen las relaciones:

$$a^{2r} = a^{n\,d + r'} = a^{n\,d} \cdot a^{r'} \equiv a^{r'} \equiv 1 \pmod{p};$$

y la última prueba que a no pertenece al exponente d: contra la hipótesis sentada.

Si d es par, la potencia $a^{\frac{d}{2}}$ producirá un resto significativo, que pertenecerá necesariamente á un divisor de $p-1$. Sea r este resto, diferente de cero, que vamos á determinar, y d' el exponente tambien diferente de cero á que pertenece; tendremos las dos congruencias consiguientes:

$$\left.\begin{aligned} a^{\frac{d}{2}} &\equiv r \\ r^{d'} &\equiv 1 \end{aligned}\right\} \text{(mod. } p\text{)}.$$

Elevando la primera á la potencia d', y teniendo en cuenta la segunda, resulta esta otra:

$$a^{\frac{d\,d'}{2}} \equiv r^{d'} \equiv 1 \text{ (mod. } p\text{)}:$$

de la cual se deduce, como a pertenece al exponente d, que $\frac{d\,d'}{2}$ debe ser múltiplo de d; y ésto no es posible sino cuando sea $d' = 0$, ó igual á 2; lo primero no puede admitirse, segun ántes dijimos; resta sólo la posibilidad de que sea $d' = 2$, y r, por lo tanto, el número que al exponente 2 pertenece; pero este número r, que pertenece al exponente 2, es $p-1$, cuya primera potencia es $\equiv -1$, y su segunda efectivamente $\equiv 1$ (mod. p); luego será por fin:

$$a^{\frac{d}{2}} \equiv -1 \text{ (mod. } p\text{)}.$$

9.ª De este teorema, en combinacion con el anterior, se desprende el siguiente:

El producto de todos los términos de un período es cóngruo con $+1$, *cuando el exponente á que el período corresponde es impar, y cóngruo con* -1, *si dicho exponente es par.*

Si el número a fuese raiz primitiva, su período comprenderia todos los números incongruentes (mod. p),

$$1,\ 2,\ 3,\ 4\ldots\ldots\ p-1.$$

cuyo producto, como $p-1$ es siempre par, á no ser $p=2$, segun acabamos de decir, será $\equiv -1 \pmod{p}$. Y aquí tenemos una nueva demostracion del teorema de Wilson (81).

Tambien es consecuencia de los teoremas anteriores, que:

10.ª *El producto de todas las raices primitivas de un número primo impar* (fuera del 3) *es siempre* $\equiv 1$.

11.ª *La suma de todos los términos de un período correspondiente á un número cualquiera es siempre* $\equiv 0$.

En efecto: designando por a un número perteneciente al exponente $d \pmod{p}$, y efectuando la division

$$(a^d - 1) : (a - 1),$$

tenemos:

$$1 + a + a^2 + \ldots\ldots + a^{d-1} \equiv \frac{a^d - 1}{a - 1} \pmod{p};$$

pero $a^d - 1$ es cóngruo con cero por hipótesis; luego

$$1 + a + a^2 + \ldots\ldots + a^{d-1} \equiv 0,$$

á no ser $a - 1$ divisible por p, ó bien $a \equiv 1 \pmod{p}$. Este caso exceptuado puede ser comprendido en el general, si llamamos tambien período á un sólo término.

12.ª *La suma de todas las raices primitivas de un número primo* p, *será congruente con* 0, *si* $p-1$ *es un producto de potencias, superiores á la primera, de números primos; y congruente con* ± 1, *cuando* $p-1$ *conste exclusivamente de factores simples.*

Ya demostramos (85) que, siendo

$$p - 1 = a^{\alpha}\, b^{\beta}\, c^{\gamma} \ldots\ldots$$

y A, B, C..... números pertenecientes á los exponentes a^{α}, b^{β}, c^{γ}...., todos los productos $A\,B\,C$..... eran raices primitivas de p. Mas, para formar estos productos, hay que combinar todos los valores de A con todos los de B, etc.; y, por tanto, la suma de todos ellos será igual (49) al producto de la suma de todos los valores de A, por la suma de todos los de B, por la suma de todos los de C, etc.: en signos se expresará dicha suma por el producto

$$(A + A' + A'' + \ldots\ldots)(B + B' + B'' + \ldots\ldots) \qquad (1)$$

cuando $A, A', A''\ldots\ldots$ y $B, B', B''\ldots\ldots$ representen los valores distintos de $A, B,$ etc.

Por consecuencia, lo que ahora debemos demostrar es que, en el supuesto de ser $\alpha = 1$ (y lo mismo podria decirse de los demás exponentes $\beta, \gamma\ldots\ldots$), la suma

$$A + A' + A'' + \ldots\ldots$$

es $\equiv -1 \pmod{p}$; y, si $\alpha > 1$, $\equiv 0 \pmod{p}$.

Ahora bien: cuando $\alpha = 1$, y A pertenece al exponente primo a, la suma de todos los números pertenecientes al mismo exponente será

$$A + A^2 + A^3 + \ldots . A^{a-1} \equiv -1 \pmod{p.};$$

puesto que (11.ª) la del período completo es

$$1 + A + A^2 + \ldots\ldots + A^{a-1} \equiv 0.$$

Y, si $\alpha > 1$, y A pertenece al exponente a^α, todos los demás números que pertenezcan al mismo exponente se obtendrán restando (84) de la série, ó período correspondiente de A,

$$1,\ A,\ A^2.\ \ldots\ldots\ A^{a^\alpha - 1}$$

todas aquellas potencias de A cuyos exponentes no sean primos con a, cuales son:

$$1,\ A^a,\ A^{2a},\ \ldots\ldots\ A^{a^\alpha - a};$$

y, como la diferencia entre las sumas de estas dos últimas séries ó períodos (4.ª y 11.ª) es congruente con cero, tambien lo será la suma de todos los números A, esto es, de todos los números pertenecientes al exponente a^α.

Así, pues, cuando $p-1$ contenga factores con exponentes α, β, γ..... que superen á la unidad, alguno de los factores, cuyo producto representa la suma de todas las raices primitivas de p, será $\equiv 0$, y tambien lo será el producto mismo, y, por lo tanto, dicha suma; y cuando $p-1$ contenga exclusivamente factores primos en su primera potencia, la suma de todas las raices primitivas será congruente con el producto de tantos factores $\equiv -1$, como sean los divisores a, b, c...., de $p-1$; esto es, $\equiv \pm 1$: segun que el número de estos divisores sea par ó impar.

Ejemplos. Las raices primitivas de 13 son 2, 6, 7, 11, cuya suma $= 26 \equiv 0$ (mod. 13); y $13-1 = 12 = 2^2 . 3$.

Las raices primitivas de 11 son 2, 6, 7, 8, cuya suma $= 23 \equiv +1$ (mod. 11); y $11-1 = 10 = 2.5$.

Las raices primitivas de 31 son 3, 11, 12, 13, 17, 21, 22, 24, cuya suma $= 123 \equiv -1$ (mod. 31), y $31-1 = 30 = 2.3.5$.

89.—*De los índices.*

En su lugar dijimos (85) que las $p-1$ potencias sucesivas de una raiz primitiva g, del número primo p,

$$g^0 = 1,\ g,\ g^2,\ g^3,\ \ldots..\ g^{p-2} \qquad (G)$$

son todas incongruentes, y que sus restos (mod. p) constituyen, por consecuencia, un sistema completo respecto de este módulo. Infiérese de aquí que cualquier número a, primo con p, por precision será congruente con una, y una sola, de las potencias (G). Si designamos, pues, por g^α esta potencia, la congruencia

$$a \equiv g^\alpha \text{ (mod. } p)$$

será siempre posible. El exponente α de la potencia de g, congruente con a, se llama *índice* de este número, y la raiz primitiva, elegida, se denomina *base*. Permaneciendo constante la base, los números incongruentes (mod. p) tendrán sus índices correspondientes, y estos índices

formarán un *sistema,* muy semejante al de los logaritmos, del cual se diferencia, sin embargo, en que las bases de los sistemas de índices sólo pueden ser las raices primitivas de un número dado (primo hasta ahora), y para base de un sistema de logaritmos puede elegirse un número cualquiera.

Determinada préviamente la base de un sistema de índices, para expresar que un número, a, es congruente con la potencia α de la base elegida, se escribe sencillamente:

$$Ind.\, a = \alpha.$$

90.—*Propiedades de los índices.*

1.ª Ya hemos indicado que dos números congruentes tienen el mismo índice, es decir que: *si se verifica la congruencia*

$$a \equiv b \,(\text{mod. } p), \quad \textit{será:} \quad Ind.\, a = Ind.\, b.$$

2.ª *Dada la congruencia*

$$c \equiv a\, b \,(\text{mod. } p).$$

se verifica tambien esta otra:

$$Ind.\, c \equiv Ind.\, a + Ind.\, b \,(\text{mod. } p - 1)$$

ó bien, abreviando, la que sigue:

$$Ind.\,(a\, b) \equiv Ind.\, a + Ind.\, b \,(\text{mod. } p - 1).$$

En efecto, siendo g la base, tenemos por definicion:

$$a \equiv g^{Ind.\, a} \,(\text{mod. } p), \quad b \equiv g^{Ind.\, b} \,(\text{mod. } p)$$

de cuyas congruencias se desprende esta otra:

$$a\,b \equiv g^{Ind.\,a\,+\,Ind.\,b} (\text{mod. } p);$$

mas, por definicion tambien, es

$$a\,b \equiv g^{Ind.\,(a\,b)} (\text{mod. } p),$$

y, por consecuencia,

$$g^{Ind.\,(a\,b)} \equiv g^{Ind.\,a\,+\,Ind.\,b} (\text{mod. } p):$$

luego (82)

$$Ind.\,(a\,b) \equiv Ind.\,a + Ind.\,b\,(\text{mod. } p-1);$$

puesto que g pertenece al exponente $p-1$.

Esta propiedad puede generalizarse para un número cualquiera de factores, y expresarse entónces así:

$$Ind.\,(a\,b\,c.....) \equiv Ind.\,a + Ind.\,b + Ind.\,c + ... (\text{mod. } p-1).$$

Y, si ahora suponemos que todos estos factores sean equivalentes al primero a, será por fin:

$$Ind.\,(a^n) \equiv n\,Ind.\,a\,(\text{mod. } p-1),$$

representando n el número de dichos factores.

3.ª *De la congruencia*

$$q \equiv \frac{a}{b} (\text{mod. } p) \quad \text{ó bien} \quad b\,q \equiv a\,(\text{mod. } p)$$

se deduce, como acabamos de ver, esta otra:

$$Ind.\,b + Ind.\,q \equiv Ind.\,a\,(\text{mod. } p-1);$$

y de aquí:

$$Ind.\left(\frac{a}{b}\right) \equiv Ind.\,a - Ind.\,b\,(\text{mod. } p-1).$$

Y por último, de la

$$r \equiv \sqrt[n]{A} \text{ (mod. } p)$$

se desprende tambien la que sigue:

$$n\,Ind.\,r \equiv Ind.\,A \text{ (mod. } p-1).$$

4.ª De las propiedades estudiadas se colige muy fácilmente la dependencia entre los índices de varios sistemas. Sean a y b dos bases diferentes, esto es, dos raices primitivas del número p; m otro número cualquiera; β y μ los índices de b y m en el sistema a; α y μ los índices de a y m en el sistema b; tendremos por definicion:

$$b \equiv a^{\beta} \text{ y } m \equiv a^{\mu}$$

$$b \equiv a^{\alpha} \text{ y } m \equiv b^{\mu'}$$

de las cuales se deducen:

$$a^{\alpha\beta} \equiv b^{\alpha} \equiv a \;\; ; \text{ y, por lo tanto: } \alpha\beta \equiv 1 \text{ (mod. } p-1);$$

$$b^{\alpha\mu} \equiv a^{\mu} \equiv b^{\mu'}; \qquad \alpha\mu \equiv \mu' \text{ (mod. } p-1)$$

$$a^{\beta\mu'} \equiv b^{\mu'} \equiv a^{\mu}, \qquad \beta\mu' \equiv \mu \text{ (mod. } p-1).$$

Luego, dado el índice β de b, en el sistema a, el índice de a en el sistema b, será $\equiv \frac{1}{\beta}$ (mod. $p-1$).

Pero, si bien un mismo número puede tener varios índices, segun bases distintas, todos ellos poseen, sin embargo, un carácter comun: el máximo divisor con $p-1$; segun se desprende de las últimas congruencias.

5.ª Es importante notar además que:

Existen dos números, $+1$ y -1, *cuyos índices son siempre los mismos cualquiera que sea la base que se adopte.*

En cuanto á la unidad positiva, en efecto, como siempre se verifica la congruencia

$$g^{p-1} = 1 = g^{0} \,(\text{mod. } p),$$

cualquiera que sea la raiz primitiva g, evidentemente será

$$Ind.\ 1 = p - 1 \equiv 0 \,(\text{mod. } p - 1):$$

lo cual quiere decir, en otros términos, que *el índice de la unidad positiva en todos los sistemas es siempre cero.*

Respecto de la unidad negativa, de la misma congruencia de Fermat, que puede tambien escribirse de este modo:

$$g^{p-1} - 1 = \left(g^{\frac{p-1}{2}} - 1\right)\left(g^{\frac{p-1}{2}} + 1\right) \equiv 0 \,(\text{mod. } p),$$

se desprende que uno por lo ménos de los dos factores incluidos en los paréntesis tiene que ser divisible por p; y, como el primero de ellos no puede serlo, porque la congruencia entónces resultante,

$$g^{\frac{p-1}{2}} \equiv 1 \,(\text{mod. } p)$$

estaria en contradiccion con la hipótesis de pertenecer g al exponente $p - 1$, habrá de serlo necesariamente el segundo, esto es:

$$g^{\frac{p-1}{2}} + 1 \equiv 0 \,(\text{mod. } p) \quad \text{ó} \quad g^{\frac{p-1}{2}} \equiv -1 \,(\text{mod. } p);$$

de cuya congruencia se infiere:

$$Ind.\ (-1) = \frac{p-1}{2};$$

ó, en lenguaje vulgar, que *el índice de la unidad negativa en todos los sistemas es siempre* $\frac{p-1}{2}$.

La aplicacion de los índices á los cálculos exije que dispongamos de *Tablas* (*) como acontece en los logaritmos. Dado el módulo 13, y tomada por base su raiz primitiva 2, una muestra de estas tablas es:

1.ª

a	1	2	3	4	5	6	7	8	9	10	11	12
Ind. a	0	1	4	2	9	5	11	3	8	10	7	6

2.ª

Ind. a	0	1	2	3	4	5	6	7	8	9	10	11
a	1	2	4	8	3	6	12	11	9	5	10	7

91.—*Uso de las tablas de índices para resolver las congruencias de primer grado.*

La resolucion de la congruencia de primer grado

$$a\,x \equiv b\,(\text{mod. } p.),$$

se reduce mediante el *Canon arithmeticus* á una simple division, y ésta, en último término, á una resta. En efecto, de la congruencia propuesta se deduce inmediatamente (90–3.ª)

$$Ind.\,x \equiv Ind.\,b - Ind.\,a\,(\text{mod. } p - 1).$$

Ejemplo. Sea la congruencia

$$5\,x \equiv 6\,(\text{mod. } 13).$$

(*) *Jacobi* publicó (Berlin—1839) unas tablas de esta especie tituladas: *Canon arithmeticus sive tabulæ, quibus exhibentur, pro singulis numeris primis vel primorum potestatibus infra* 1000, *numeri ad datos indices et indices ad datos numeros pertinentes.*

Tomando por base de los índices la raiz primitiva 2, del módulo 13, tendremos segun la tabla 1.ª:

$$Ind.\, x \equiv Ind.\, 6 - Ind.\, 5 \equiv 5 - 9 \equiv -4 \equiv 8 \,(\text{mod. } 12):$$

y, como 8 es el índice de 9, segun la tabla 2.ª, será finalmente:

$$x \equiv 9 \,(\text{mod. } 13).$$

Este método para resolver las congruencias de primer grado, que parece sólo aplicable, á primera vista, á las de módulo primo, puede serlo tambien á las de módulo compuesto, como se concibe desde el momento que reflexionemos que una congruencia de esta especie puede descomponerse en una série de congruencias cuyos módulos sean primos.

Sea, pues, la congruencia

$$a\,x \equiv b \,(\text{mod. } k),$$

en la cual supondremos a primo con k. Si p representa un factor primo contenido en $k = p\,k'$, resolveremos primeramente la congruencia, segun este factor primo,

$$a\,x \equiv b \,(\text{mod. } p);$$

y obtendremos la solucion, por ejemplo:

$$x \equiv \alpha \,(\text{mod. } p) \quad \text{ó bien} \quad x = \alpha + p\,x',$$

siendo x' un número entero. La congruencia propuesta, sustituyendo en ella por x su valor hallado, se convierte en esta otra:

$$p\,a\,x' \equiv b - a\,\alpha \,(\text{mod. } k);$$

y, reparando que su segundo miembro, $b - a\,\alpha$, es divisible por p, y, puede, en consecuencia, ser representado por $b'\,p$, en la siguiente:

$$a\,x' \equiv b' \,(\text{mod. } k')$$

cuyas raices son las mismas de la primera. Resolviendo nuevamente esta última congruencia respecto de un factor primo p', contenido en k', y así prosiguiendo, llegaremos á una finalmente de cuya raiz, por sustituciones sucesivas, obtendremos las de la propuesta.

92.—*De las raices primitivas de una potencia superior á la primera de un número primo impar, ó del duplo de tal potencia.*

Supongamos, de acuerdo con este epígrafe, que sea

$$k = p^{\pi} \text{ ó } = 2p^{\pi},$$

y, por lo tanto, en ambos casos: $\varphi(k) = (p-1)p^{\pi-1}$.

En otro lugar demostramos (80) que de todos los individuos del sistema completo de restos (mod. k) solamente satisfacian á la congruencia de Euler

$$x^{\varphi(k)} \equiv 1 \text{ (mod. } k),$$

los $\varphi(k)$ números primos con k é inferiores á este número. Aplicando las definiciones y principios anteriormente (84) establecidos, pudiéramos tambien decir ahora que, si el número a pertenece al exponente d (mod. $k = p^{\pi}$ ó $2p^{\pi}$), y claro es entónces que a necesariamente es primo con k, los restos de las potencias

$$1,\ a,\ a^2 \ldots\ a^{d-1}$$

son todos incongruentes (mod. k); y, si designamos por

$$1,\ d',\ d'' \ldots\ d-1$$

los números inferiores y primos con d, todos los números pertenecientes al exponente d serán congruentes (mod. k) con los restos de las potencias

$$a,\ a^{d'},\ a^{d''} \ldots\ a^{d-1}.$$

Si g representa una raiz primitiva de k, los restos de las potencias

$$1,\ g,\ g^2\ .\ \ldots\ g^{\varphi(k)-1}$$

son diferentes entre sí, y coinciden con los números primos con k é inferiores á este número; y los restos de aquellas cuyos exponentes tengan comun con $\varphi(k)$ el máximo divisor $\delta = \varphi(k) : d$, serán precisamente los números que pertenecen al exponente d (mod. k).

Mas todas estas leyes que, por analogía hasta cierto punto, hemos repetido, se confirmarán directamente en cuanto manifestemos las relaciones que guardan con las otras á que los módulos primos sencillos obedecen.

Para proceder con método en este estudio comenzaremos por demostrar el siguiente

Léma. Si h representa un entero cualquiera, y $\pi \geqq 1$ un número entero y positivo, se verificará siempre la congruencia

$$\left(1 + hp^{\pi}\right)^p \equiv 1 + hp^{\pi+1} \left(\text{mod. } p^{\pi+2}\right) \qquad (1).$$

En efecto, desarrollando su primer miembro por la fórmula conocida del binomio, tendremos la igualdad:

$$\left(1 + hp^{\pi}\right)^p = 1 + p\,hp^{\pi} + \frac{p(p-1)}{1\,.\,2} h^2 p^{2\pi} +$$

$$+ \frac{p(p-1)(p-2)}{1\,.\,2\,.\,.\,3} h^3 p^{3\pi} + \ldots\ldots$$

ó bien, parándonos en el tercer término del desarrollo, la congruencia

$$\left(1 + hp^{\pi}\right)^p \equiv 1 + hp^{\pi+1} + \frac{p-1}{2} h^2 p^{2\pi+1} \left(\text{mod. } p^{3\pi}\right);$$

de la cual, teniendo en cuenta que el cociente completo $(p-1) : 2$ es entero por ser p número impar, y que las potencias $2\pi + 1$ y 3π de p son divisibles por la potencia $\pi + 2$ del mismo número, se deduce inmediatamente la (1) que procurábamos demostrar.

a.—Refiriéndonos primeramente al caso en que el módulo sea una potencia superior á la primera de un número primo impar, admitamos que g sea efectivamente una raiz primitiva, no del módulo p^{π}, sino de la potencia inmediatamente superior $p^{\pi+1}$, esto es, un número perteneciente al exponente $\varphi\left(p^{\pi+1}\right)=(p-1)p^{\pi}$, respecto de $p^{\pi+1}$; y designemos por d el exponente, desconocido por el pronto, á que el mismo g pertenece respecto del módulo p^{π}. De la equivalencia que expresa esta última hipótesis,

$$g^{d}=1+hp^{\pi},$$

se deduce, segun el lema, la congruencia

$$g^{dp}\equiv 1\left(\text{mod. } p^{\pi+1}\right):$$

y de aquí, como g pertenece al exponente

$$\varphi\left(p^{\pi+1}\right)=(p-1)p^{\pi},$$

que dp tiene que ser divisible por $(p-1)p^{\pi}$, y, por lo tanto, d *divisible* por $(p-1)p^{\pi-1}=\varphi\left(p^{\pi}\right)$; mas, por pertenecer g al exponente d, segun el módulo p^{π}, debe ser tambien dicho exponente, d, *divisor* de

$$\varphi\left(p^{\pi}\right)=(p-1)p^{\pi-1}:\ \text{luego}\ \ d=\varphi\left(p^{\pi}\right);$$

y, por consecuencia, g raiz primitiva de p^{π}, ó bien

$$g^{(p-1)p^{\pi-1}}=1+hp^{\pi}.$$

De esta última igualdad se infiere además que el número h es primo con p; porque, si fuera divisible por p, la congruencia entónces resultante,

$$g^{(p-1)p^{\pi-1}}\equiv 1\left(\text{mod. } p^{\pi+1}\right),$$

estaria en contradiccion con el supuesto establecido de ser g raiz primitiva del módulo $p^{\pi+1}$.

Y de cuanto queda probado se concluye que toda raiz primitiva g del módulo $p^{\pi+1}$ lo es tambien del módulo p^{π}; y, extendiendo esta conclusion hasta la primera potencia de p, que:

Toda raiz primitiva, g, de una potencia cualquiera, p^{π}, de un número primo impar, es tambien raiz primitiva de p, es decir, satisface á la equivalencia

$$g^{p-1} = 1 + hp,$$

en la cual es h primo con p, y por lo tanto, el binomio $g^{p-1} - 1$ no es divisible por p^2.

Admitamos ahora, á la inversa, que g sea efectivamente una raiz primitiva del módulo p^{π}, esto es, un número que satisfaga á la equivalencia

$$g^{\varphi(p^{\pi})} = 1 + hp^{\pi}.$$

en la cual sea precisamente h primo con p; y designemos por d el exponente á que el mismo g pertenece, respecto del módulo $p^{\pi+1}$.

De la congruencia consiguiente,

$$g^{d} \equiv 1 \pmod{p^{\pi+1}},$$

se desprende, segun acabamos de demostrar, esta otra:

$$g^{d} \equiv 1 \pmod{p^{\pi}};$$

y de aquí, como g es por hipótesis raiz primitiva de p^{π}, que d tiene que ser *divisible* por $\varphi(p^{\pi})$; más, por pertenecer g al exponente d, respecto del módulo $p^{\pi+1}$, debe ser tambien dicho exponente d *divisor* de $\varphi(p^{\pi+1}) = p\varphi(p^{\pi})$: luego necesariamente habrá de ser $d = \varphi(p^{\pi})$ ó igual á $\varphi(p^{\pi+1})$. Lo primero es inadmisible; puesto

que hemos calificado el número h de primo con p; queda, por consecuencia, lo segundo, á saber: $d = \varphi(p^{\pi+1})$: y esto prueba que g es tambien raiz primitiva de $p^{\pi+1}$, ó que satisface á la congruencia

$$g^{(p-1)p^{\pi}} \equiv 1 \pmod{p^{\pi+1}};$$

de la cual se deduce que en la igualdad consiguiente,

$$g^{(p-1)p^{\pi}} = (1 + hp^{\pi})^{p} = 1 + h'p^{\pi+1};$$

el número h' tampoco puede ser divisible por p.

Razonando como en el caso anterior, se concluye que:

Toda raiz primitiva g de un número primo impar p, para la cual no sea el binomio $g^{p-1} - 1$ divisible por p^2, es también raiz primitiva de cualquiera potencia más elevada de p.

De este resultado se infiere que, si entre las raices primitivas de un número primo impar p, que ya sabemos hallar (86), probamos que existen algunas g, para las cuales la diferencia $g^{p-1} - 1$ no sea divisible por p^2, no sólo habremos al mismo tiempo demostrado que existen realmente raices primitivas de potencias más elevadas de p, sino que podremos además determinar cuáles y cuántas son en suma. Representemos por f una raiz primitiva de p; la expresion $g = f + px$ comprenderá todas las raices congruentes con f, y, aplicándole la fórmula del binomio, dará evidentemente:

$$g^{p} \equiv f^{p} \pmod{p^2}.$$

Por ser f raiz primitiva de p, será el binomio $f^{p-1} - 1$, ó bien $f^{p} - f$, divisible por p, mas no por p^2; por consecuencia, si designamos por f' el resto (mod. p) del cociente entero $(f^{p} - f) : p$, podremos establecer la igualdad

$$\frac{f^{p} - f}{p} = f' + np$$

de la cual se deduce esta otra:

$$f^p - f = f'p + np^2, \text{ ó la congruencia } f^p \equiv f + f'p \pmod{p^2}.$$

Poniendo en lugar de f^p su congruente g^p, y restando despues de esta última congruencia, así modificada, la expresion abreviada, escrita arriba, de las raices primitivas congruentes con la raiz f, obtendremos la que sigue:

$$g^p - g \equiv p(f' - x) \pmod{p^2}:$$

la cual patentiza que sólo podrá ser $g^p - g$ divisible por p^2 cuando $f' - x$ sea divisible por p, en cuyo supuesto tambien se verificará la congruencia, $g \equiv g^p \equiv f^p \pmod{p^2}$. Fuera de esta excepcion, $g^p - g$, ó bien $g^{p-1} - 1$, no será divisible por p^2; y g, por lo tanto, como demostramos há poco, representará entónces una raiz primitiva de cualquier potencia de p.

Habiendo ya explicado cómo se hallan las raices primitivas de una potencia superior de p, conocidas las de su primera potencia, para saber ahora cuántas son, basta recordar que el número de las raices f distintas, de p, es $\varphi(p-1)$; y, como cada una de estas produce $(p-1)$ raices g, incongruentes $\pmod{p^2}$, resulta que:

Todas las raices primitivas de potencias superiores á la primera de un número primo impar, p, constituyen los individuos comprendidos en las $(p-1)\varphi(p-1)$ clases distintas de números incongruentes respecto del módulo p^2.

Ejemplo. Las raices primitivas del módulo 7 son 3 y 5: todos los números comprendidos en las dos séries abreviadas

$$3 + 7x \quad \text{y} \quad 5 + 7x,$$

en las cuales puede recibir x todos los valores sucesivos desde 1 hasta 6, serán tambien raices primitivas de potencias superiores de 7, á excepcion de aquellos que sean congruentes $\pmod{7^2}$ con 31 ó 19, por ser

$$3^7 \equiv 31 \pmod{49} \quad \text{y} \quad 5^7 \equiv 19 \pmod{49}.$$

b.—El caso en que el módulo sea el duplo de una potencia cualquiera de un número primo impar, se refiere al anterior mediante la proposicion siguiente:

Toda raiz primitiva de una potencia, p^{π}, *de un número primo impar* p, *lo es tambien del duplo*, $2p^{\pi}$, *de dicha potencia, y reciprocamente; y toda raiz primitiva, par, de* p^{π}, *más ó ménos este módulo, da un resultado que es raiz primitiva tambien de* $2p^{\pi}$.

Designemos por x primeramente un número impar, y por d el exponente á que pertenece x respecto del módulo p^{π}. Por hipótesis tendremos:

$$x^{d} \equiv 1 \pmod{p^{\pi}}$$

y, por ser x impar,

$$x^{d} \equiv 1 \pmod{2}:$$

y, de consiguiente (61–6.ª)

$$x^{d} \equiv 1 \pmod{2p^{\pi}}.$$

Si hiciéramos la suposicion de que otro exponente $d' < d$ verificara la congruencia

$$x^{d'} = 1 \pmod{2p^{\pi}},$$

como de ésta se deduce la siguiente

$$x^{d'} \equiv 1 \pmod{p^{\pi}},$$

se concluiria, contra la hipótesis, que no pertenecia x al exponente d: luego efectivamente pertenece x al exponente d segun el módulo $2p^{\pi}$. Si admitimos ahora que sea x par, y d el exponente á que pertenece respecto del módulo p^{π}, de la congruencia evidente,

$$x \pm p^{\pi} \equiv x \pmod{p^{\pi}}.$$

se desprende esta otra:

$$(x \pm p^{\pi})^{d} \equiv 1 \pmod{p^{\pi}}$$

y, por ser $x \pm p^{\pi}$ impar, la que sigue:

$$(x \pm p^{\pi})^{d} \equiv 1 \pmod{2}$$

de las cuales, como 2 y p^{π} son primos entre sí, resulta (61-6.ª) finalmente:

$$(x \pm p^{\pi})^{d} \equiv 1 \pmod{2p^{\pi}};$$

probándose, como antes, que efectivamente pertenece $x \pm p^{\pi}$ al exponente d segun el módulo $2p^{\pi}$.

Ahora bien, como en el supuesto de ser x raiz primitiva, el exponente á que pertenece entónces $\pmod{2p^{\pi}}$ es (56-Cor.)

$$\varphi(2p^{\pi}) = \varphi(p^{\pi}) = (p-1)p^{\pi-1},$$

conclúyese que, si x es raiz primitiva de p^{π} lo será tambien de $2p^{\pi}$, y viceversa.

93.—*De los índices.*

Representando por g una raiz primitiva de p^{π}, y haciendo para mayor sencillez

$$\varphi(p^{\pi}) = c,$$

repetiremos ya con plena razon, á semejanza de lo demostrado (85) para los módulos primos impares, que las potencias (comenzando por la $g^{c} \equiv 1 = g^{0}$),

$$g^{0}, g^{1}, g^{2}, g^{3}, \ldots\ldots g^{c-1} \qquad (G)$$

son todas incongruentes $(\text{mod. } p^{\pi})$, y constituyen, por lo tanto, un sistema completo de números incongruentes con exclusion de los divisibles por p. Por consecuencia, si designamos por a un número cualquiera no divisible por p, entre las potencias g existirá necesariamente una que verifique la congruencia

$$a \equiv g^{\alpha} (\text{mod. } p^{\pi})$$

y cuyo exponente α sea un individuo de los infinitos que comprende la clase de números $\equiv \alpha (\text{mod. } c)$. Uno cualquiera de estos exponentes se llama *índice* del número a para la *base* g; lo cual se expresa en signos de este modo:

$$Ind.\ a \equiv \alpha (\text{mod. } c).$$

Así, cuando el exponente α reciba sucesivamente los valores de un sistema completo de restos (mod. c), los valores correspondientes de a formarán un sistema tambien completo de números incongruentes (módulo p^{π}) y primos con p^{π}.

Las operaciones con estos índices se hallan sometidas á las mismas leyes que ya explicamos (90) al hablar de las raices primitivas para los números simples, esto es, para el caso $\pi = 1$; de modo que no repetiremos sobre esta materia sino que ahora son:

$$Ind.\ (1) \equiv 0 \quad \text{é} \quad Ind.\ (-1) \equiv \frac{1}{2} c (\text{mod. } c).$$

Conocido el índice del número a, no es difícil determinar el exponente d, á que pertenece dicho número segun el módulo p^{π}. En efecto, de la congruencia ó definicion

$$a \equiv g^{Ind.\ a} (\text{mod. } p^{\pi}),$$

se deduce esta otra:

$$a^{d} \equiv g^{d\ Ind.\ a} (\text{mod. } p^{\pi});$$

y, como por hipótesis,

$$a^d \equiv 1 \pmod{p^\pi},$$

síguese que $d\ Ind.\ a$ debe ser divisible por $\varphi(p^\pi) = c$. Mas para que ésto suceda, si designamos por δ el máximo comun divisor de los números $Ind.\ a$ y c, es necesario que d sea un múltiplo del cociente $c:\delta$; y es claro que el mínimo múltiplo de este cociente es él mismo, é igual, por consecuencia, al exponente d á que el número a pertenece.

Si suponemos ahora que $\delta = 1$, el exponente hallado $c:\delta$ se convierte en c, y los números $Ind.\ a$ y c serán primos entre sí; y entónces el número a pertenecerá al exponente c, ó será raiz primitiva de p^π, siempre que el exponente $Ind.\ a$ sea primo con c: de donde se sigue que el número de las raices primitivas, incongruentes $\pmod{p^\pi}$, es igual al conjunto de los números primos é inferiores á $c = \varphi(p^\pi)$, existentes en la série de los exponentes de las potencias (G),

$$0,\quad 1,\quad 2,\ldots\ldots c-1,$$

cuyo número sabemos se expresa por

$$\varphi\, c = \varphi\,\varphi(p^\pi) = \varphi\Big[(p-1)p^{\pi-1}\Big].$$

94.—*De las raices primitivas de una potencia cualquiera del número* 2.

Evidentemente, para la primera potencia del módulo 2, todo número impar puede considerarse como raiz primitiva; y ya vimos (83) que, para el módulo $2^2 = 4$, el número $3 \equiv -1 \pmod{4}$ satisfacia tambien á la definicion de raiz primitiva. Si, pues, -1 es raiz primitiva de 4, segun acabamos de decir en el párrafo precedente, todo número a, primo con 2, ó impar, será congruente (mod. 4) con una potencia de -1, ó bien satisfará á la congruencia

$$a \equiv (-1)^\alpha \pmod{4}, \qquad (1$$

en la cual será el exponente α par ó impar, ó lo que es igual, $\equiv 0 \pmod 2$ ó $\equiv 1 \pmod 2$, segun que a tenga la forma $4n+1$ ó $4n-1$, ó, en otros términos, segun que a sea $\equiv 1 \pmod 4$ ó $\equiv -1 \pmod 4$. Hasta aquí el módulo 2 no se aparta, en la cuestion de las raices primitivas, de los números primos impares; pero no sucede lo mismo cuando el exponente λ del módulo 2 es igual ó superior á 3, en cuyos casos se verifica la ley (83)

$$a^{2^{\lambda-2}} = a^{\frac{1}{2}\varphi(2^\lambda)} \equiv 1 \pmod{2^\lambda},$$

cierta, además, evidentemente para $\lambda = 3$; puesto que siempre es

$$a^2 = (4n \pm 1)^2 = 16n^2 \pm 8n + 1 \equiv 1 \pmod{2^3};$$

y, por tanto, segun el lema (92), para todos los valores superiores de λ; y la cual prueba que, para el módulo 2^λ, siendo $\lambda \geq 3$, no existen raices primitivas en el sentido que asignamos á esta palabra.

Algunos autores (*), sin embargo, llaman por analogía raices primitivas de 2^λ á los números pertenecientes al exponente $\frac{1}{2}\varphi(2^\lambda)$, segun el módulo 2^λ. Sin alterar nosotros el significado de las denominaciones ya admitidas, veamos si existen efectivamente números de esta especie, y la semejanza que pueda existir entre estos números y las raices primitivas, verdaderas, de los otros módulos primos.

Ensayemos para esto el número 5. De la congruencia evidente

$$5 \equiv 1 + 2^2 \pmod{2^3},$$

por elevaciones sucesivas al cuadrado, se deducen las que siguen:

$$5^2 \equiv 1 + 2^3 \pmod{2^4}$$

$$5^{2^2} \equiv 1 + 2^4 \pmod{2^5}$$

$$5^{2^3} \equiv 1 + 2^5 \pmod{2^6}$$

$$\cdots\cdots\cdots\cdots\cdots$$

(*) Schwarz.—Zahlen, Theorie, §. 14.

y, en general:

$$5^{2^{\lambda-3}} \equiv 1 + 2^{\lambda-1} \pmod{2^{\lambda}};$$

pero nunca

$$5^{2^{\lambda-3}} \equiv 1 \pmod{2^{\lambda}}.$$

De aquí se infiere que el exponente á que el número 5 pertenece segun el módulo 2^{λ}, no será divisor de $2^{\lambda-3}$, y como tiene que serlo de $2^{\lambda-2}$, es este mismo número precisamente.

Esto probado, si designamos por b el número $\frac{1}{2}\varphi(2^{\lambda}) = 2^{\lambda-2}$, para mayor brevedad, repitiendo lo que acerca de los otros módulos expusimos, diremos ahora tambien que los b números

$$5^0,\ 5^1,\ 5^2,\ \ldots\ldots\ 5^{b-1}$$

son todos incongruentes $\pmod{2^{\lambda}}$; y que lo propio acontece con los siguientes:

$$(-5^0),\ (-5)^1,\ (-5)^2,\ \ldots\ldots\ (-5)^{b-1}.$$

Siendo los primeros, todos $\equiv 1 \pmod 4$, y los segundos $\equiv -1 \pmod 4$, forman juntos un sistema de $\varphi(2^{\lambda})$ números impares, incongruentes $\pmod{2^{\lambda}}$: luego, si representamos por a un número impar, puede éste sin inconveniente expresarse por la congruencia

$$a \equiv (-1)^{\alpha} 5^{\beta} \pmod{2^{\lambda}}, \qquad (2)$$

en la cual α y β designan cualquiera de los restos respectivamente de los módulos 2, y $2^{\lambda-2} = b$. Así, cuando α reciba todos los valores de un sistema completo de restos (mod. 2), y β, independientemente de α, los de otro sistema completo de restos (mod. b), los correspondientes de a formarán tambien un sistema completo de nú-

meros incongruentes $(\text{mod. } 2^\lambda)$, y primos con 2^λ, esto es, impares. Por consecuencia, un número impar cualquiera será congruente $(\text{mod. } 2^\lambda)$ con un valor solo del producto

$$(-1)^\alpha 5^\beta,$$

cuyos exponentes α y β son los verdaderos *índices* en esta ocasion de dicho número, sometidos á las mismas leyes que ya conocemos y no hay necesidad de repetir nuevamente. Solo advertiremos ahora que será $a \equiv \pm 1$, ó $\equiv \pm 3 \pmod 8$, segun que β sea par ó impar; puesto que el número $5 \equiv -3 \pmod 8$, y todas las potencias pares de 3 son $\equiv 1 \pmod 8$, y las impares $\equiv 3 \pmod 8$. Nótese que la congruencia (2) que representa los números impares, en el supuesto de ser $\lambda \gtrless 3$, comprende tambien el caso en que sea $\lambda = 2$; porque entónces el número $b = \frac{1}{2}\varphi$ (4) de los valores de β se reduce á uno solo, que es la unidad; y con ésto, y teniendo presente que $5 \equiv 1 \pmod 4$, la congruencia mencionada se convierte en la siguiente ya conocida (1):

$$a \equiv (-1)^\alpha \pmod 4.$$

Y no solamente este caso $\lambda = 2$, sino que además la forma (2) puede extenderse á todos los números primos con el módulo 2^λ, áun para los valores de λ inferiores á 2, $\lambda = 0$ y $\lambda = 1$; porque para estos valores comprende aquella una clase sola de números, y los exponentes α y β, por consecuencia, no pueden recibir sino un solo valor. Haciendo, pues, $b = 1 = m$, siempre que $\gamma = 0$ ó $= 1$, y $m = 2$, $\beta = \frac{1}{2}\varphi(2^\lambda)$, cuando $\lambda \gtrless 2$, podremos afirmar en general que la congruencia (2) representará todos los números incongruentes y primos con el módulo 2^λ, sin excepcion ninguna, si los exponentes α y β recorren independientemente un sistema completo de restos cada uno, respecto de los módulos m y b.

95.—*De las raices primitivas de un número cualquiera.*

Sea el módulo

$$k = 2^{\lambda} p^{\pi} p'^{\pi'} \ldots\ldots$$

en cuya forma representan $p, p' \ldots\ldots$ números primos diferentes, y $\lambda, \pi, \pi', \ldots\ldots$ números enteros positivos.

Fácil es comprender, despues de lo dicho en los párrafos precedentes, que un número cualquiera N, primo con k, debe satisfacer al sistema de congruencias:

$$N \equiv (-1)^{\alpha} 5^{\beta} \pmod{2^{\lambda}}$$

$$N \equiv g^{\nu} \pmod{p^{\pi}}$$

$$N \equiv g'^{\nu'} \pmod{p'^{\pi'}}$$

$$\ldots\ldots\ldots\ldots\ldots$$

en las cuales $g, g' \ldots\ldots$ designan raices primitivas de los módulos $p^{\pi}, p'^{\pi'} \ldots\ldots$ ó bien (93) de $p^2, p'^2 \ldots\ldots$

Conservando para los números m y b la significacion que les dimos al fin del último párrafo, y haciendo para mayor brevedad

$$\varphi(p^{\pi}) = c, \ \varphi(p'^{\pi'}) = c' \ldots\ldots$$

los índices ó exponentes $\alpha, \beta, \nu, \nu' \ldots\ldots$ podrán recibir independientemente los valores de un sistema completo de restos cada uno, respecto de los módulos $m, b, c, c' \ldots\ldots$ A cada sistema de estos valores corresponderá (72) una clase determinada de números N, respecto de k, y primos con este módulo; y el número total de estos sistemas, ó, lo que es lo mismo, el producto de todos los valores que son susceptibles de recibir los índices $\alpha, \beta, \nu, \nu' \ldots\ldots$ será igual al número de clases de los números primos con k, esto es:

$$m\, b\, c\, c' \ldots\ldots = \varphi(k).$$

Conocidos los índices α, β, ν, ν' ..... para un número N cualquiera, determinado, es muy sencillo calcular el exponente á que pertenecerá este número respecto del módulo k; pues tal exponente es el mínimo comun múltiplo de los exponentes á que dicho número pertenece, segun los módulos 2^{λ}, p^{π} $p'^{,\pi'}$ ....., y divisor además, por lo tanto, del mínimo comun múltiplo de los números m, b, c, c' .....

Tambien pudiéramos deducir facilmente de este resultado la demostracion que anticipamos (83) acerca de la existencia de las raices primitivas; pero, sin detenernos en más pormenores, pasemos ya á tratar de la resolucion de las congruencias binomias, para lo cual tenemos los fundamentos necesarios, comenzando por las de módulo primo á que se reducen en último término las referentes á otro módulo cualquiera.

96.—*Resolucion de la congruencia binomia de módulo primo. Enunciado del problema.*

Sabemos que la forma general de esta congruencia es

$$a x^{\mu} \equiv b \,(\text{mod. } p):$$

la cual, segun demostramos (77), puede convertirse en la de forma ordinaria

$$x^{\mu} \equiv D \,(\text{mod. } p). \qquad (1)$$

Mas con la advertencia que D se supone siempre primo con p; pues el caso en que fuese, por el contrario, $D \equiv 0$ (mod. p), y, por consecuencia, $x \equiv 0$ (mod. p), carece de importancia y sin inconveniente le omitimos. Tambien debemos notar que la congruencia (1) en el caso de que fuera $n > p$, sería equivalente á otra cuyo grado representaria el resto de n (mod. $p-1$), lo cual es evidente.

Esto sentado, la cuestion que debemos estudiar abraza dos partes. Primera: *¿es posible siempre la congruencia propuesta?* ó en otros términos: *¿existen* (entre 0 y p naturalmente) *números x que, dados n y D, la satisfagan?* Segunda: *si estos números x existen, ¿cuántos son y cómo se hallan?*

De las proposiciones generales (Cap. II) podrian inmediatamente deducirse las condiciones para que la congruencia (1) tuviese soluciones enteras, y el número de estas soluciones, mucho más cuando ya hicimos aplicacion de las mismas á un caso particular (80). Pero, una vez que ya está explicada la doctrina de los índices, preferimos, siguiendo á Gauss (*), utilizarla primeramente en resolver la cuestion planteada; porque así creemos facilitar tambien la inteligencia de lo que despues diremos acerca de la misma.

97.—*Resolucion por el Cánon Arithmeticus.*

Tomando índices de la congruencia propuesta

$$x^n \equiv D \,(\text{mod. } p), \qquad (1)$$

tendremos (89):

$$n\ Ind.\, x \equiv Ind.\, D \,(\text{mod.}\, p-1);$$

ó bien, si designamos por ξ y γ respectivamente los índices, respecto de una raiz cualquiera de p, de los números x y D,

$$n\xi \equiv \gamma \,(\text{mod. } p-1): \qquad (2)$$

de donde se sigue que el problema cuya solucion buscamos se reduce á determinar todas las raices incongruentes ξ de la congruencia (2); porque á cada una de estas raices corresponderá una sola de la congruencia (1), ó un sólo valor de x. Pero la congruencia de primer grado (2) será posible (68) si se verifica precisamente la condicional

$$\gamma = Ind.\, D \equiv 0 \,(\text{mod. } \delta) \qquad (3)$$

cuyo módulo δ representa el máximo comun divisor de los números n y $p-1$; y entónces admitirá δ soluciones incongruentes (mod. $p-1$). Luego en general:

(*) D. A., §§ 60 y 68.—Dirichlet.—Zahlen Theorie h. von Dedekind, §. 31.

Si δ *representa el máximo comun divisor del grado* n *de la congruencia* (1) *y del número* $p-1$, *esta congruencia será posible, y admitirá* δ *soluciones incongruentes* (mod. p), *sólo cuando se verifique la congruencia* (3).

Expresando por $\sqrt[n]{D}$ (mod. p), á semejanza de lo que hicimos en las ecuaciones de primer grado (69—*E*), una raiz cualquiera de la congruencia (1), podremos decir que $\sqrt[n]{D}$ tendrá un solo valor real, ó δ valores incongruentes (mod. p), segun que n y $p-1$ sean primos entre sí, ó contengan el máximo divisor δ; pero con la condicion indispensable en este último caso de que se verifique la condicion (3); porque, de lo contrario, $\sqrt[n]{D}$ no representaría valor real ninguno.

Ejemplo. Sea la congruencia

$$x^8 = 3 \,(\text{mod. } 13), \qquad (1)$$

de la cual se deduce inmediatamente esta otra:

$$8\, Ind.\, x \equiv Ind.\, 3 \,(\text{mod. } 12).$$

Tomando por base la raiz primitiva 2 del módulo 13, en la tabla (90-1.ª) encontramos $Ind.\, 3 = 4$, y la congruencia

$$8\, Ind.\, x \equiv 4 \,(\text{mod. } 12), \qquad (2)$$

posible por ser 4 el máximo comun divisor de 8 y 12, admitirá 4 soluciones. Para encontrarlas simplifiquémosla, y resulta la siguiente:

$$2\, Ind.\, x \equiv 1 \,(\text{mod. } 3),$$

y de aquí:

$$Ind.\, x \equiv 2 \,(\text{mod. } 3),$$

ó las cuatro soluciones:

$$Ind.\, x \equiv 2,\ 5,\ 8,\ 11 \,(\text{mod. } 12).$$

Buscando ahora en la tabla (2.ª) los números correspondientes á los índices 2, 5, 8, 11, hallamos por último:

$$x \equiv 4,\ 6,\ 9,\ 7 \pmod{13}.$$

Con el auxilio de las *Tablas* ó *Cánon Arithméticus* todas las cuestiones que al principio planteamos quedan pronta y satisfactoriamente resueltas; mas no debemos olvidar, sin embargo, que este método es indirecto, y además que no siempre tendremos á nuestra disposicion las tablas que requiere. Preciso es, por lo tanto, idear otro medio para conocer cuándo será posible una congruencia binomia sin acudir á los índices, primero, y para encontrar, despues, todas sus raices.

98.—*Resolucion directa.*

Bien pronto se concibe que no será muy difícil hallar lo que deseamos, cuando ya el criterio de la posibilidad de una congruencia binomia lo hemos determinado, segun el método anterior, prescindiendo completamente de especificar y elejir la raiz primitiva del módulo á que los índices de la incógnita y el segundo miembro de aquella se referian. Sea cualquiera la raiz primitiva g del número primo p, el índice γ del segundo miembro D, dijimos, en la congruencia *posible*,

$$x^n \equiv D \pmod{p},$$

tiene que ser múltiplo de un divisor δ de $p-1$, esto es, debe tener la forma $h\delta$, siendo h entero. De la congruencia que define este índice de D,

$$D \equiv g^{h\delta} \pmod{p},$$

elevándola á la potencia $\frac{p-1}{\delta}$, se desprende esta otra:

$$D^{\frac{p-1}{\delta}} \equiv g^{h(p-1)} \equiv 1 \pmod{p}.$$

Y recíprocamente, si se verifica esta última,

$$D^{\frac{p-1}{\delta}} \equiv 1 \,(\text{mod. } p),$$

el índice γ de D tiene que ser múltiplo de δ; pues de la definicion

$$D \equiv g^{\gamma} \,(\text{mod. } p)$$

se deduce, por igual proceder que ántes, la congruencia

$$D^{\frac{p-1}{\delta}} \equiv g^{\frac{\gamma}{\delta}(p-1)} \equiv 1 \,(\text{mod. } p),$$

la cual prueba, como g pertenece al exponente $p-1$, ó es raiz primitiva de p, que debe ser entero el cociente $\gamma : \delta$; y, por lo tanto, γ múltiplo de δ.

De donde se concluye efectivamente que:

Si δ *representa el máximo comun divisor del grado* n *de la congruencia* (1) *y del número* $p-1$, *esta congruencia admitirá* δ *soluciones, ó ninguna, segun que se verifique, ó no se verifique la condicional*

$$D^{\frac{p-1}{\delta}} \equiv 1 \,(\text{mod. } p);$$

en cuya conclusion para nada figuran ya las raices primitivas ni los índices.

Sin mentar los índices siquiera, sino admitiendo únicamente que δ sea un factor de $p-1$, podemos demostrar que la posibilidad de la congruencia

$$x^{\delta} \equiv D \,(\text{mod. } p), \qquad (1)$$

exije como condicion indispensable que se verifique esta otra:

$$D^{\frac{p-1}{\delta}} \equiv 1 \,(\text{mod. } p). \qquad (2)$$

y, recíprocamente, que, si ésta se verifica, es posible aquélla y admite δ raices. En efecto, elevando la (1) á la potencia $\frac{p-1}{\delta}$ tendremos:

$$x^{p-1} \equiv D^{\frac{p-1}{\delta}} \pmod{p};$$

y de aquí, como x es primo con p, por el teorema de Fermat, la (2); y está demostrada la proposicion directa. Para demostrar la recíproca restemos la congruencia supuesta,

$$D^{\frac{p-1}{\delta}} \equiv 1 \pmod{p},$$

de la de Fermat, y resultará:

$$x^{p-1} - D^{\frac{p-1}{\delta}} = \left(x^{\delta}\right)^{\frac{p-1}{\delta}} - D^{\frac{p-1}{\delta}} \equiv 0 \pmod{p},$$

ó bien

$$\left(x^{\delta}\right)^{\frac{p-1}{\delta}} - D^{\frac{p-1}{\delta}} \equiv x^{p-1} - 1 \pmod{p}.$$

Mas el primer miembro de esta última congruencia contiene el divisor $x^{\delta} - D$, y lo mismo, por consecuencia, sucede con el segundo: luego (80) la congruencia

$$x^{\delta} \equiv D \pmod{p}$$

es posible, y admite realmente δ soluciones.

Ejemplos. La congruencia

$$x^{21} \equiv 2 \pmod{31},$$

es posible, porque se verifica la condicional

$$2^{10} = 1024 \equiv 1 \pmod{31}.$$

La congruencia

$$x^2 \equiv -1 \,(\text{mod. } p),$$

admitirá dos soluciones reales, siempre que p sea de la forma $4m+1$, en cuyo supuesto se verifica la condicional

$$(-1)^{2m} \equiv 1 \,(\text{mod. } 4m+1);$$

pero no admitirá ninguna, cuando sea p de la forma $4m+3$; porque entónces

$$(-1)^{2m+1} = -1.$$

De este último ejemplo se desprende el siguiente teorema:

Siendo p un número primo de la forma $4m+1$, es posible hallar un cuadrado x^2 que, sumado con la unidad, produzca un resultado divisible por p; y no es posible hallarlo cuando p tenga la forma $4m-1$.

99.—*Número de restos potenciales incongruentes.*

Conocido el criterio de la posibilidad de una congruencia binomia y cuántas soluciones admite, cuando es posible, directamente, sin el auxilio de los índices, conviene antes de investigar cuáles sean estas soluciones, contestar á la pregunta siguiente:

¿Cuántos son los restos potenciales, incongruentes, ó los números D que satisfacen á la congruencia posible

$$x^n \equiv D \,(\text{mod. } p)?$$

La condicion antes determinada para que un número D sea resto potencial de otro x, respecto del módulo p, nos da la contestacion que buscamos; pues ella manifiesta que los números D representan todas las raices de la congruencia

$$x^{\frac{p-1}{\delta}} \equiv 1 \,(\text{mod. } p):$$

la cual, como el máximo comun divisor de su grado $\frac{p-1}{\delta}$, y del número $p-1$, es el exponente mismo de x, es siempre posible, y el número de sus raices incongruentes D es, por consecuencia, $\frac{p-1}{\delta}$.

Infiérese de este resultado, que sustituyendo por x en la congruencia dada todos los valores posibles, esto es, todos los términos del sistema completo de restos (mod. p),

$$1,\ 2,\ 3,\ \ldots..\ (p-1),$$

solamente hallaremos $\frac{p-1}{\delta}$ entre ellos que den restos diferentes, elevados á la potencia n; por cuya razon los $p-1$ restos de p pueden distribuirse en $\frac{p-1}{\delta}$ clases, cada una de las cuales contendrá δ individuos que representarán las δ soluciones que admite la congruencia propuesta para cada uno de los $\frac{p-1}{\delta}$ valores incongruentes (mod. p) que es susceptible de recibir su segundo miembro D.

Si n y $p-1$ fuesen primos entre sí, y entónces $\delta = 1$, los restos de las potencias del sistema completo (mod. p),

$$1,\ 2^n,\ 3^n,\ 4^n,\ \ldots..\ (p-1)^n,$$

serian todos diferentes, y coincidirian, prescindiendo del órden, con la série de números

$$1,\ 2,\ 3,\ 4,\ \ldots..\ (p-1),$$

cuyos individuos representan en este caso las clases de los valores que podria tomar D.

Ejemplo. En la congruencia

$$x^3 \equiv D \pmod{31},$$

cuyo grado 3 es un divisor de 30, si sustituimos por x el sistema completo de restos (mod. 31)

$$1,\ 2,\ 3,\ 4,\ \ldots\ldots\ 30,$$

solamente encontraremos $30 : 3 = 10$ que den restos diferentes; de modo que los 30 restos de 31 pueden distribuirse en 10 clases, cada una de las cuales comprenderá 3 números que darán igual resto. Así sucede en efecto: los 10 valores incongruentes que puede recibir D son los siguientes:

$$1,\ 2,\ 4,\ 8,\ 15,\ 16,\ 23,\ 27,\ 29,\ 30.$$

Dan el resto 1 los tres valores de x, 1, 5, 25; el resto 2, los valores 4, 7, 20; el 4, los valores 16, 18, 28; los valores 2, 10, 19 el 8; 17, 22, 23 el 15; 8, 9, 14 el 16; 12, 21 29 el 23; 3, 13, 15 el 27; 11, 24, 27 el 29; y por último, los valores de x, 6, 26, 30, el resto $30 \equiv -1$.

Será en vano buscar para x valores cuyas terceras potencias diesen los restos 3, 5, 6, 7, 9, 10..... etc. (mod. 31).

100.—*Modo de hallar directamente las raices.*

Réstanos todavía, para dar por terminada la cuestion que venimos estudiando, explicar cómo se halla directamente un valor de la expresion $\sqrt[n]{D}$.

Para esto conviene recordar precisamente que, tanto al hablar de los exponentes á que pertenecen los números, como despues del número de las raices de una congruencia, hemos indicado que tales exponentes y el grado de esta congruencia se suponian divisores del módulo ménos la unidad. De aquí se colige que debemos enseñar ante todo cómo se reducen, si es posible, todas las expresiones $\sqrt[n]{D}$ (mod. p), á otras equivalentes en las cuales sea n divisor de $p - 1$.

Fácil es encontrar la reduccion que deseamos. En efecto, sea x un valor cualquiera que satisface á la congruencia

$$x^n \equiv D \,(\text{mod. } p).$$

y d otro valor que verifica esta otra:

$$n\,d \equiv \delta \,(\text{mod. } p-1).$$

Elevando la primera á la potencia d tendremos:

$$x^{n\,d} \equiv D^{d},$$

y, en virtud de la segunda:

$$x^{n\,d} \equiv x^{\delta};$$

y, por lo tanto,

$$x^{\delta} \equiv D^{d} \,(\text{mod. } p):$$

de lo cual se deduce que todo valor de $\sqrt[n]{D}$ lo será tambien de $\sqrt[\delta]{D^{d}}$; y, por consecuencia, que, si $\sqrt[n]{D}$ tiene valores reales, equivaldrá á la expresion $\sqrt[\delta]{D^{d}}$ que tendrá tantos como aquella.

Sea la congruencia, por ejemplo,

$$x^{21} \equiv 2 \,(\text{mod. } 31).$$

El máximo comun divisor δ de 21 y 30 es 3; y un valor de d, deducido de la congruencia auxiliar

$$21\,d \equiv 3 \,(\text{mod. } 30),$$

es 3: luego si $\sqrt[21]{2}$ (mod. 31) tiene valores reales equivaldrá á la expresion $\sqrt[3]{2^{3}} = \sqrt[3]{8}$, ó bien la congruencia dada á esta otra:

$$x^{3} \equiv 8 \,(\text{mod. } 31),$$

cuyo grado es un divisor de 30, y sus raices 2, 10 y 19.

Con esta trasformacion no tenemos ya necesidad de estudiar sino aquellas congruencias (mod. p) cuyos grados sean divisores de $p-1$.

Supongamos que el grado n de la congruencia

$$x^n \equiv D \,(\text{mod. } p)$$

sea efectivamente un divisor de $p-1$. Entónces, si $D \equiv 1$, y a un valor de x perteneciente al exponente n (que ya sabemos hallar), las potencias

$$1,\ a,\ a^2 \ \ldots\ldots\ a^{n-1}$$

comprenderán todas las raices de la congruencia

$$x^n \equiv 1 \,(\text{mod. } p).$$

Pero, si D no fuese congruente con la unidad, y z representa un valor conocido de $\sqrt[n]{D}$, ó raiz de la congruencia propuesta, todas sus raices estarian dadas por los restos (mod. p) de los productos

$$z,\ z\,a,\ z\,a^2,\ z\,a^{n-1};$$

porque, en primer lugar, todos ellos la satisfacen: lo cual es evidente en cuanto uno cualquiera $z\,a^r$, por ejemplo, se eleve á la potencia n, y veamos que se convierte entónces en $z^n . a^{nr}$, y como $a^n \equiv 1$, segun ántes admitimos, resulta efectivamente $z^n \equiv D$; y, en segundo, son todos diferentes entre sí (63), y tantos además, como raices ó valores puede admitir la expresion $\sqrt[n]{D}$.

Síguese de lo dicho que para determinar todas las raices de la congruencia

$$x^n \equiv D \,(\text{mod. } p),$$

es preciso conocer préviamente un valor x que pertenezca al exponente n, y despues otro z que satisfaga á esta congruencia.

¿Cómo encontraremos, pues, este valor z que verifique la congruencia

$$z^n \equiv D \text{ (mod. } p)? \qquad (\alpha)$$

Si llegáramos á conocer, caso de que exista, un número congruente con cualquier potencia de D, tal como $z \equiv D^r$, ya tendríamos lo que buscamos; porque entónces sería tambien $z^n \equiv D^{nr} \equiv D$: y la cuestion, por consecuencia, se reduce á determinar el exponente r. Este exponente debe satisfacer á la congruencia $D^{nr} \equiv D$, ó bien á la condicional equivalente (82)

$$nr \equiv 1 \text{ (mod. } d); \qquad (\beta)$$

en la cual d representa el exponente á que el número D pertenece. Mas la congruencia $nr \equiv 1$ (mod. d) será posible, cuando n sea primo con d, en cuyo supuesto se deduciria $r \equiv \frac{1}{n}$ (mod. d); é imposible siempre (68) que n y d contengan algun divisor comun: luego en este último caso es inútil buscar valor ninguno de z que sea congruente con una potencia de D, porque tal valor sólo puede existir en el primero.

Conocido el exponente d á que el número D pertenece, la cuestion está resuelta; pero, si no le conociéramos, poco ó nada habríamos logrado. Réstanos, por consecuencia, explicar cómo procederemos cuando no conozcamos dicho exponente d.

Supongamos para esto, como siempre, que sea posible la congruencia que se trata de resolver, y designemos por y una cualquiera de sus raices, de modo que tengamos ciertamente:

$$y^n \equiv D \text{ (mod. } p).$$

Elevando esta congruencia á la potencia $\frac{p-1}{n}$ resulta la siguiente:

$$y^{p-1} \equiv D^{\frac{p-1}{n}} \text{ (mod. } p);$$

y, teniendo en cuenta el teorema de Fermat, esta otra:

$$D^{\frac{p-1}{n}} \equiv 1 \text{ (mod. } p\text{)}:$$

la cual prueba que $\frac{p-1}{n}$ debe ser divisible por d. Esto sentado, si fuese $\frac{p-1}{n}$ primo con n, la congruencia condicional (β) sería posible para el módulo $\frac{p-1}{n}$; una raiz suya, r, la satisfaria tambien segun el módulo d, divisor de $\frac{p-1}{n}$; y con esto habríamos hallado, por consecuencia, el exponente r de D que necesitamos. Si $\frac{p-1}{n}$ y n no son primos entre sí, suprimiremos del primero todos los factores primos comunes á los dos, y el cociente resultante $\frac{p-1}{nq}$, donde q representa el producto de todos estos factores, ya será primo con n: luego, en el supuesto de que se verifique la condicion antes establecida de ser d primo con n, será tambien d primo con q, y divisor, por lo tanto, del cociente $\frac{p-1}{nq}$; y esto prueba que el valor de r, deducido de la congruencia posible $nr \equiv 1$, segun el módulo $\frac{p-1}{nq}$, será una solucion de la misma segun el módulo d, divisor del anterior, y el exponente, tambien, del número D, que buscamos. Segun se ve, lo que tratamos de hallar, mediante el procedimiento explicado, es un número que pueda reemplazar para nuestro objeto al d que nos es desconocido; mas conviene notar que en el curso de la explicacion, al suponer que $\frac{p-1}{n}$ y n no eran primos entre sí, ni un momento hemos admitido que dejara de cumplirse la condicion primera de ser n primo con d, sin cuyo requisito fueran erróneas las deducciones subsiguientes. Así que de someterse meramente á las reglas

prescritas, sin asegurarse de si se verifica ó no aquella condicion, podríamos encontrar para z un valor cuya potencia n no fuese congruente con D; lo cual manifestaría que no se verificaba. Pero falso y todo el valor de z, hallado de esta manera, nos sirve, sin embargo, para obtener mas pronto el verdadero: porque si designamos por v un valor cualquiera de la expresion $\sqrt[n]{D : z^n}$, esto es, que verifique la congruencia $v^n \equiv D : z^n \pmod{p}$, será evidentemente $(v\,z)^n \equiv D$.

Un par de ejemplos acabarán de poner en claro las explicaciones que anteceden.

Ejemplo. 1.° Sea la congruencia

$$x^3 \equiv 31 \pmod{37}:$$

en la cual valen las letras antes usadas: $n = 3$, $D = 31$, $p = 37$, $p - 1 = 36$, $\frac{p-1}{n} = 12$, $q = 3$. Segun el procedimiento general, debe verificarse la congruencia $3r \equiv 1 \pmod{4}$ que da $r = 3$, y, por consecuencia, $z \equiv D^r = 31^3 \equiv 6 \pmod{37}$. Pero efectivamente:

$$z^3 = 6^3 \equiv 31 \pmod{37}:$$

luego, si conocemos los valores a de la congruencia

$$a^3 \equiv 1 \pmod{37},$$

ó bien un número a perteneciente al exponente 3 (mod. 37), los que buscamos serán z, $z\,a$, $z\,a^2$. Los valores de la expresion $\sqrt[3]{1}$ (mod. 37), son 1, 10, 26: los cuales, multiplicados por $z \equiv 6$, producen para los de $\sqrt[3]{31}$ (mod. 37), los siguientes: 6, 60, 156, ó bien los restos 6, 23, 8, respecto del módulo 37.

2.° Sea la congruencia

$$x^2 \equiv 3 \pmod{37},$$

para la cual son: $n = 2$, $D = 3$, $p = 37$, $p - 1 = 36$, $\frac{p-1}{n} = 18$, $q = 2$. En este caso debe verificarse la congruencia $2r \equiv 1 \pmod{9}$, de donde resulta $r = 5$, y, por lo tanto, $z \equiv 3^5 \equiv 21 \pmod{37}$; pero aquí $z^2 = 21^2$ no es $\equiv 3$, sino $\equiv 34$; lo cual indica que 21 es un valor falso de z, que nos sirve, sin embargo, para determinar el de la expresion $D : z^n = 3 : 21^2 = 3 : 34 \pmod{37}$, que es $36 \equiv -1$ (módulo 37); y, por éste, los del radical $\sqrt[n]{D : z^n} = \sqrt{3 : 34} \equiv \sqrt{-1}$ (mod. 37), ó bien, los de x en la congruencia $x^2 \equiv -1 \pmod{37}$, que son ± 6, de los cuales resultan para x los siguientes: $\pm 6 \cdot 21 \equiv \pm 15$.

101.—*Resolucion de la congruencia binomia para un módulo cualquiera.*

Resuelto completamente el problema para el caso de un módulo primo impar, pudiéramos ahora considerarlo respecto de un módulo que fuese una potencia cualquiera de un número primo impar, ó el duplo de tal potencia; en seguida para el módulo igual á una potencia cualquiera del número 2; y, por último, en el caso general de ser el módulo un número cualquiera. Pero el escaso interes relativo de estudiar así paso á paso la cuestion, por una parte, y el tiempo ya empleado en la investigacion de las raices propias y primitivas referentes á cada uno de estos módulos, por otra, nos dispensan buenamente de insistir sobre tantos pormenores.

Diremos, sin embargo, recapitulando y ampliando los resultados obtenidos para las congruencias de módulo primo que:

La congruencia de módulo cualquiera k,

$$x^n \equiv D \pmod{k}, \qquad (1)$$

será posible siempre que se verifique la condicional

$$D^{\frac{\varphi(k)}{\delta}} \equiv 1 \pmod{k}, \qquad (2)$$

y entónces admitirá δ *soluciones enteras, si* δ *representa el máximo comun divisor del grado* n *de la congruencia y del número* $\varphi(k)$.

Si este máximo comun divisor δ fuese igual á la unidad, y, por consecuencia, n y $\varphi(k)$ primos entre sí, la congruencia (1) admitiria una solucion única, á saber:

$$z \equiv D^{r},$$

estando el exponente r determinado por la de primer grado

$$nr \equiv 1 \text{ (mod. } d),$$

solamente posible (68) cuando n sea primo con su módulo d, que expresa el exponente á que D pertenece (mod. k.)

Admitida la posibilidad de la congruencia propuesta, podremos trasformarla en otra

$$x^{\nu} \equiv D \text{ (mod. } k),$$

cuyo grado sea un divisor de $\varphi(k)$; y, si por x sustituimos en esta última los $\varphi(k)$ números primos con k é inferiores á este número:

$$1,\ k',\ k'',\ \ldots\ldots k-1$$

los restos de las potencias

$$1,\ k'^{\nu},\ k''^{\nu},\ \ldots\ldots (k-1)^{\nu}$$

podrán distribuirse en $\varphi(k) : \nu$ grupos, cada uno de los cuales comprenderá ν números que produzcan igual resto.

Despues de esta breve digresion á propósito de la semejanza entre las leyes á que las congruencias de números primos y compuestos obedecen, hé aquí ahora cómo se procede en la resolucion general de la congruencia para un módulo cualquiera.

Sea la congruencia en su forma mas general

$$f(x) \equiv 0 \text{ (mod. } A\,B\,C\ldots\ldots) \qquad (1)$$

en la cual representan $A, B, C, \ldots\ldots$ números primos entre sí dos á dos.

La resolucion de esta congruencia puede siempre reducirse á la del sistema

$$\begin{aligned} f(x) &\equiv 0 \pmod{A} \\ f(x) &\equiv 0 \pmod{B} \\ f(x) &\equiv 0 \pmod{C} \\ &\ldots\ldots\ldots\ldots \end{aligned} \qquad (2)$$

En efecto: en primer lugar, es claro que toda raiz de la congruencia (1) debe satisfacer tambien á todas las congruencias del sistema (2); y, por consecuencia, será imposible aquella siempre que lo sea alguna de estas últimas. Recíprocamente: si a representa una raiz cualquiera de la congruencia $f(x) \equiv 0 \pmod{A}$; b una raiz de la congruencia $f(x) \equiv 0 \pmod{B}$; c otra de la congruencia $f(x) \equiv 0 \pmod{C}$; etc.; y se determina (72) un número x que satisfaga al sistema de congruencias

$$\begin{aligned} x &\equiv a \pmod{A} \\ x &\equiv b \pmod{B} \\ x &\equiv c \pmod{C} \\ &\ldots\ldots\ldots\ldots \end{aligned} \qquad (3)$$

tendremos evidentemente:

$$\begin{aligned} f(x) \equiv f(a) &\equiv 0 \pmod{A} \\ f(x) \equiv f(b) &\equiv 0 \pmod{B} \\ f(x) \equiv f(c) &\equiv 0 \pmod{C} \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

y, como A, B, C, ... son primos entre sí dos á dos (72), tambien la congruencia

$$f(x) \equiv 0 \pmod{A\,B\,C\ldots\ldots}.$$

Es decir, que todo número x que satisfaga al sistema (3) es una raiz de la congruencia (1); y, por lo tanto, que el problema propuesto se reduce á encontrar dicho número x. Pero todos estos números x, que satisfacen al sistema (3), son (72) congruentes (mod. $A\,B\,C$.....), y representan una sola clase; por cuya razon dicho sistema de congruencias (3) nos sirve exclusivamente para determinar una sola raiz de la congruencia (1).

Ahora bien, si designamos por

λ el número de todos los valores incongruentes de a (mod. A)

μ id. id. de b (mod. B)

ν id. id. de c (mod. C).

.....

podremos formar $\lambda\,\mu\,\nu$..... sistemas diferentes (3), mediante los cuales determinaremos otras tantas raices de la congruencia (1); y, como cualquiera raiz de esta última debe satisfacer, segun ya dijimos, á todas las congruencias (2), y ser congruente, por consecuencia, con un valor determinado de a (mod. A), con otro de b (mod. B), con un tercero de c (mod. C), etc., resulta que la congruencia propuesta (1) no contendrá raices diferentes de las que los $\lambda\,\mu\,\nu$..... sistemas (3) produzcan; y, por lo tanto, que el número de todas sus raices incongruentes (módulo $A\,B\,C$.....) será $\lambda\,\mu\,\nu$ precisamente.

Ejemplo. Sea la congruencia

$$11\,x^{20} \equiv -13 \text{ (mod. } 72).$$

De la congruencia auxiliar

$$11\,y \equiv 1 \text{ (mod. } 72),$$

se deduce

$$y = -13:$$

y, multiplicando por este número la congruencia propuesta, y restando de los productos el módulo 72, resulta ya reducida á la forma ordinaria, la siguiente:

$$x^{20} \equiv 25 \text{ (mod. } 72), \qquad (1)$$

que puede descomponerse en el sistema:

$$x^{20} \equiv 25 \equiv -2 \pmod{9},$$

$$x^{20} \equiv 25 \equiv 1 \pmod{8}. \qquad (2)$$

Para determinar una raiz de la primera de éstas rebajaremos su grado hasta el resto mínimo respecto de $\varphi(9) = 6$, y tendremos:

$$x^2 \equiv -2 \pmod{9},$$

la cual nos da las dos raices

$$a \equiv \pm 4.$$

La segunda congruencia, referente al módulo $8 = 2^3$, para la cual es $\frac{1}{2}\varphi(2^3) = 2^{3-2} = 2$, contiene las mismas raices reales que la siguiente:

$$x^2 \equiv 1 \pmod{8},$$

que admite las cuatro raices enteras

$$b \equiv 1,\ 3,\ -3,\ -1.$$

Síguese de esto que $\lambda = 2$, $\mu = 4$, y $\lambda\mu = 8$.
De las congruencias auxiliares (72)

$$8\alpha \equiv 1 \pmod{9} \quad \text{y} \quad 9\beta \equiv 1 \pmod{8}$$

se deducen: $\alpha \equiv -1$ y $\beta \equiv +1$;

y, por consecuencia, los números x que satisfacen al sistema (3) serán en general:

$$x \equiv -8a + 9b \pmod{72}.$$

de cuya expresion, sustituyendo por a sus dos valores $+4$ y -4, y por b, independientemente de a, sus cuatro correspondientes, 1, 3, -3, -1, resultan los ocho sistemas:

$$\begin{array}{ll} x \equiv -8.4+9.1 & x \equiv 8.4+9.1 \\ \quad +9.3 & \quad +9.3 \\ \quad -9.3 & \quad -9.3 \\ \quad -9.1 & \quad -9.1, \end{array}$$

ó, lo que es igual, los ocho valores de x,

$$x \equiv -23,\ -5,\ -59,\ -41,\ 41,\ 59,\ 5,\ 23 \text{ (mod. 72)},$$

ó bien, tomando exclusivamente los restos mínimos positivos,

$$x \equiv 5,\ 13,\ 23,\ 31,\ 41,\ 49,\ 59,\ 67 \text{ (mod. 72)}.$$

102.—*Observacion.*

Si reflexionamos un poco acerca de las leyes consignadas en las páginas anteriores notaremos que, tanto para determinar los valores de la incógnita en la congruencia

$$x^n \equiv D \text{ (mod. } k),$$

como para cerciorarnos de si esta congruencia es posible, dados su grado y su segundo miembro, y áun para prefijar cuántos valores puede recibir éste dentro de los límites de su posibilidad, representa el módulo el papel más interesante. En verdad que esta circunstancia no debe sorprendernos cuando ya clasificamos y representamos los números con relacion á estos tipos, y de la forma ó estructura de los módulos dedujimos las propiedades comunes á los individuos comprendidos en aquellas clases. Pero lo que, despues de esto, debe llamar nuestra atencion

es que, al tratar de las congruencias binomias, sólo por incidencia, en ejemplos ó casos particulares, hayamos discutido las formas del módulo correspondiente, que hemos supuesto, una vez establecido, invariable, al paso que minuciosamente consideramos las que pudieran afectar los otros dos términos ó partes componentes de la congruencia binomia: su incógnita y su segundo miembro, en cada una de las secciones que constituyen la teoría precedente. Para que esta fuese completa, por consecuencia, sería preciso admitir que el módulo goza de igual variabilidad que los otros términos, respecto del mismo congruentes; y entónces el problema, que bajo ciertas condiciones hemos considerado hasta ahora, debiera ampliarse hasta comprender estas dos partes: una, cuyo objeto fuese determinar las formas de los restos potenciales para un módulo dado, y las raices de las congruencias correspondientes á cada uno de aquellos restos; y otra en la cual se tratase de caracterizar las formas convenientes de los módulos para que ciertos números dados pudieran ser restos potenciales de aquellos. Con esta reciprocidad é independencia alternativas entre las formas, unas veces variables y otras constantes, de los restos y de los módulos, se completaria la doctrina de las congruencias binomias; mas para llegar á este grado de generalidad resta mucho que hacer todavía. Sin embargo, aunque no tan de lleno, concretándonos á las cuadráticas, podemos afirmar tambien que poseemos ya una teoría completa, bien definida, en conformidad con el significado y representacion que asignamos al número, ejemplo y acabado modelo del caso general antes enunciado, y de suma trascendencia por sus aplicaciones, y porque, si no las resuelve, señala las dificultades hasta hoy invencibles del problema total, sirviendo al mismo tiempo de guia para lograrlo. Expondremos á continuacion, con la posible brevedad, la teoría mencionada.

CAPITULO IV.

De las congruencias de segundo grado.

103.—*Restos cuadráticos.*

Toda congruencia de segundo grado con una incógnita sabemos que puede reducirse á la binomia

$$x^2 \equiv D \text{ (mod. } k\text{)}, \qquad (1)$$

en la cual se supone siempre á D primo con k.

Si esta congruencia es posible, ya dijimos (82) que el número D se llamaba *resto cuadrático* del módulo k: y, si no fuere posible, D tomaria el nombre de *no-resto cuadrático* del mismo módulo: advirtiendo para lo sucesivo que el calificativo de *cuadrático* suele omitirse siempre que no surja de tal omision duda ni ambigüedad ninguna.

Puesto que los cuadrados de dos números congruentes (mod. k) son tambien congruentes, y, por otra parte, la incógnita x y el número D en la congruencia (1) no pueden en realidad recibir valores diferentes de los términos que constituyen el sistema completo de restos del módulo k, un número cualquiera, congruente con un cuadrado cualquiera, deberá serlo por precision con el cuadrado de alguno de los $k-1$ términos del mencionado sistema de restos de k: es decir, que los individuos comprendidos en cada una de las $k-1$ clases, en que los números no divisibles por k pueden segun k distribuirse, serán todos *restos*, ó todos *no-restos* cuadráticos del módulo k.

La teoría completa de estos restos, segun ya en general indicamos en el último párrafo, debe constar de dos partes principales:

1.ª *Dado el módulo k, hallar los restos D, y las raices ó soluciones de la congruencia* (1) *para cada uno de estos restos.*

2.ª *Dado el número D, hallar los módulos k para los cuales sea D resto cuadrático.*

PRIMERA PARTE.—104.—*Carácter de un número.*

Supongamos ante todo que el módulo k sea la primera potencia de un número primo impar p; y así excluimos desde luego el número 2, en atencion á que todo número, no divisible por 2, es siempre congruente con el cuadrado de 1 (único resto de 2), y, por lo tanto, resto cuadrático de 2. Si, en conformidad con lo que poco antes dijimos, del sistema completo de restos de p,

$$1,\ 2,\ 3,\ \ldots\ldots\ (p-1),$$

elevamos al cuadrado los siguientes:

$$1,\ 2,\ 3,\ \ldots\ldots\ \frac{p-1}{2},$$

los restos de los cuadrados resultantes serán todos incongruentes; porque, admitiendo que dos cualesquiera de ellos, r^2 y s^2 por ejemplo, fuesen congruentes (mod. p), su diferencia (59)

$$r^2 - s^2 = (r+s)(r-s)$$

tendria que ser divisible por p; y, de consiguiente, alguno de sus dos factores $r+s$, ó $r-s$: lo cual es imposible por ser ambos menores que p. Luego los $\frac{1}{2}(p-1)$ cuadrados de la mitad de los términos del sistema completo de restos de p, producen efectivamente $\frac{1}{2}(p-1)$ restos incongruentes, y como los cuadrados de los términos de la otra mitad,

$$\frac{p+1}{2},\ \frac{p+3}{2},\ \ldots\ldots\ (p-1),$$

dan los mismos restos que los anteriores, puesto que siempre,

$$(p-r)^2 = p^2 - 2pr + r^2 \equiv r^2 \pmod{p},$$

resulta finalmente que

Entre los $(p-1)$ *restos de* p *existen* $\frac{1}{2}(p-1)$ *que son restos cuadráticos de* p, *esto es, la mitad; y otros tantos, por consecuencia, que son no-restos del mismo* p.

Demostrado que de los $(p-1)$ restos de p, la mitad solamente pueden ser restos cuadráticos, veamos ahora si existe un medio seguro de distinguirlos y caracterizarlos.

Para esto comenzaremos por dar una definicion que nos permitirá despues abreviar nuestros razonamientos. Así como llamamos (88) simplemente *sócios* á dos números cuyo producto fuese congruente con la unidad (mod. p), diremos aquí que son *sócios en* D (*) dos números, y, en general, todo par de números cuyo producto sea congruente con D (mod. p). Segun esta definicion, designando por r, s, los números sócios en D, se verificará la congruencia

$$rs \equiv D \pmod{p},$$

de la cual, como es de primer grado, y r, s son menores que p, se desprende que, dado un número r del sistema de restos de p,

$$1,\ 2,\ 3,\ 4,\ \ldots\ldots\ p-1, \qquad (1)$$

siempre existirá otro s en la misma série, y uno solo que sea sócio suyo en D. En general, estos dos números sócios en D son diferentes; pero tambien pueden ser iguales, esto es, un número x sócio de sí mismo, y entónces la congruencia anterior de primer grado se convierte en la de segundo

$$x^2 \equiv D \pmod{p}, \qquad (2)$$

cuyas dos raices son precisamente los números de que hablamos, y de los cuales es D resto cuadrático (mod. p).

(*) Generalmente se llaman tambien estos números *conjugados*.

Ahora bien, si suponemos que los números sócios en D son diferentes, en cuyo caso la última congruencia es imposible, y por lo tanto, D es no-resto (mod. p), como para ser idénticas dos parejas de números sócios basta que contengan uno solo comun, los términos del sistema de restos (1) podrán distribuirse en $\frac{1}{2}(p-1)$ pares de sócios en D, y su producto, por consecuencia, será:

$$1.\ 2.\ 3.\ \ldots\ (p-1) \equiv D^{\frac{p-1}{2}} \pmod{p}. \qquad (3)$$

Si admitimos, por el contrario, que la congruencia (2) sea posible, y ρ represente un individuo del sistema (1) que la satisfaga, existirá otro tambien σ con la misma propiedad que el primero ρ. En efecto, olvidémonos de que la congruencia (2) admite dos raices: de la congruencia basada en la existencia hipotética del número σ,

$$\sigma^2 \equiv \rho^2 \pmod{p},$$

se deduce que la diferencia

$$\sigma^2 - \rho^2 = (\sigma + \rho)(\sigma - \rho),$$

tiene que ser divisible por p; y, de consiguiente, como ρ y σ son distintos y ambos menores que p, que $\sigma + \rho$ tiene que ser divisible por p, para lo cual, dadas las condiciones de ρ y σ, es indispensable que $\sigma + \rho = p$. De esta igualdad se desprende que $\sigma = p - \rho$; y, puesto que $(p-\rho)^2 = p^2 - 2p\rho + \rho^2 \equiv \rho^2 \equiv D \pmod{p}$, resulta efectivamente probada la realidad, supuesta al principio, del número σ, y que éste vale $p - \rho$. Separando, por un momento, esta pareja ρ y $p - \rho$, cuyo producto es $\rho(p-\rho) \equiv -\rho^2 \equiv -D$, de los $(p-1)$ números del sistema (1), los $(p-3)$ restantes pueden distribuirse en $\frac{1}{2}(p-3)$ parejas de sócios, diferentes; y el producto de estas parejas de sócios, diferentes, por el de la separada antes, esto es, el producto de todos los números del sistema (1), será por fin:

$$1.\ 2.\ 3.\ \ldots\ (p-1) \equiv -D^{\frac{p-1}{2}} \pmod{p}. \qquad (4)$$

La imposibilidad ó posibilidad de la congruencia (2) nos ha conducido respectivamente á las congruencias (3) y (4); pero es necesario añadir que existe un caso para el cual dicha congruencia (2) es siempre posible: aquel en que sea $D = 1 = 1^2$, y entónces admite evidentemente las dos soluciones, 1, y -1 ó $p-1$. La congruencia (4) para este valor particular de D se trasforma en la siguiente:

$$1.\ 2.\ 3.\ \ldots\ldots\ (p-1) \equiv -1 \pmod{p},$$

que es la de Wilson; y comparando esta congruencia con la (4), y despues con la (3), resultan estas otras:

$$D^{\frac{p-1}{2}} \equiv +1 \pmod{p} \quad \text{y} \quad D^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

las cuales expresan respectivamente las condiciones del número D para ser resto ó no resto cuadrático del módulo primo p.

Esta propiedad de ser el número D resto ó no-resto del módulo p, se conoce con el nombre de *carácter* (*) de dicho número D; y se expresa, además de por las dos últimas congruencias, por el símbolo debido á Legendre (**)

$$\left(\frac{D}{p}\right) = +1 \quad \text{y} \quad \left(\frac{D}{p}\right) = -1;$$

de manera que siempre podremos establecer la congruencia

$$D^{\frac{p-1}{2}} \equiv \left(\frac{D}{p}\right) \pmod{p}.$$

Si el número D fuese un producto m de varios factores $a\,b\,c\ldots\ldots$, como ninguno de éstos será divisible por el número primo p si su producto no lo fuese, de la igualdad

$$(a\,b\,c\ldots\ldots)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \cdot c^{\frac{p-1}{2}} \ldots\ldots$$

(*) Euleri Comm. Arithm., t. I, pág. 260 y 516, aunque no claramente expreso.
(**) Théorie des Nombres, 3.ª ed., t. I, p. 197.

se deduce que *dicho producto* $m = a\,b\,c\,\ldots\ldots$ *será resto ó no-resto de* p, *segun que el número de sus factores, no-restos de* p, *sea par ó impar.*

Esta ley, segun el símbolo de Legendre, se expresa en forma de ecuacion de este modo:

$$\left(\frac{a\,b\,c\,\ldots\ldots}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\left(\frac{c}{p}\right)\ldots\ldots$$

El carácter, pues, de un producto depende de los caracteres de sus factores.

En virtud de que los números congruentes (mod. p) tienen respecto de este módulo igual carácter, si se verifica la congruencia

$$m \equiv n \,(\text{mod. } p),$$

es cierta la igualdad

$$\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right).$$

Finalmente, otra propiedad de este mismo símbolo es la que representa la igualdad evidente

$$\left(\frac{m}{p}\right)\left(\frac{m}{p}\right) = (\pm 1)^2 = +1.$$

105.—*Trasformacion del carácter precedente.*

El carácter ó criterio de Euler para conocer si un número D, no divisible por el número primo p, es resto ó no-resto del segundo, puede trasformarse muy ventajosamente para nuestras ulteriores investigaciones (*).

(*) Gauss, Theorematis arithmetici demonstratio nova. Werke, t. II.

Formemos los productos de D por la série de números

$$1,\ 2,\ 3,\ \ldots\ldots\ \tfrac{1}{2}(p-1),$$

y designemos respectivamente por

$$r_1,\ r_2,\ r_3\ \ldots\ldots\ r_{\frac{1}{2}(p-1)},$$

los $\frac{1}{2}(p-1)$ restos, segun p, de los productos así formados,

$$D,\ 2D,\ 3D\ \ldots\ldots\ \tfrac{1}{2}(p-1)D.$$

Como D es primo con p, todos los restos r, serán (63) significativos (ninguno es 0), diferentes entre sí, y menores que p.

Separemos ahora estos restos en dos secciones: una que comprenda los mayores que $\frac{1}{2}p$, los cuales representaremos por

$$a_1,\ a_2,\ a_3,\ \ldots\ldots\ a_\mu, \qquad (A)$$

cuyo conjunto es μ; y otra en la que estén incluidos los menores que $\frac{1}{2}p$, expresados por

$$b_1,\ b_2,\ b_3,\ \ldots\ldots\ b_\lambda, \qquad (B)$$

en número de λ: y es evidente que los complementos á p de los μ restos (A),

$$p-a_1,\ p-a_2,\ p-a_3\ \ldots\ldots\ p-a_\mu,$$

son tambien diferentes, y están comprendidos, como los términos de la série (B), entre los límites 0 y $\frac{1}{2}p$. Mas, aunque así sea, los términos de la última série no coincidirán con los de la anterior; pues si

se verificase la igualdad $p - a = b$ entre uno cualquiera de los términos complementarios $p - a$, y otro, b, de los de la série (B), se deduciria de ella inmediatamente: $b + a = p \equiv 0 \pmod{p}$; y designando por AD y BD los múltiplos de D que dan los restos a y b, tambien:

$$AD + BD = (A + B)D \equiv 0 \pmod{p};$$

y de aquí, como D es primo con p, que $A + B$ sería divisible por p: lo cual es imposible por ser los dos, A y B, menores que $\frac{1}{2}p$.

Siendo, por consecuencia, diferentes los μ números complementarios, arriba escritos, de los λ de la série (B), resulta que el conjunto, $\lambda + \mu = \frac{1}{2}(p-1)$, de los unos y los otros,

$$p - a_1,\ p - a_2,\ p - a_3,\ \ldots\ p - a_\mu,\ b_1,\ b_2,\ b_3,\ \ldots\ b_\lambda.$$

cuyos valores se hallan comprendidos entre 0 y $\frac{1}{2}p$ (con exclusion de estos límites), no puede ser sino el de los $\frac{1}{2}(p-1)$ números

$$1,\ 2,\ 3,\ \ldots\ \tfrac{1}{2}(p-1):$$

y, por lo tanto, que el producto de los primeros es igual al de los segundos, á saber:

$$(p - a_1)\cdot(p - a_2)\cdot\ldots\ (p - a_\mu)\cdot b_1\cdot b_2\cdot\ldots\ b_\lambda = 1.2.3\ldots\ \tfrac{1}{2}(p-1).$$

De esta igualdad, separando los múltiplos de p, se desprende la congruencia

$$(-1)^\mu\, a_1\, a_2\ \ldots\ a_\mu\cdot b_1\, b_2\ \ldots\ b_\lambda \equiv 1.2.3\ldots\ \tfrac{1}{2}(p-1) \pmod{p}:$$

y de esta otra, evidente,

$$D \,.\, 2D \,.\, 3D \ldots\ldots \tfrac{1}{2}(p-1)D = 1 \,.\, 2 \,.\, 3 \ldots\ldots \tfrac{1}{2}(p-1)D^{\frac{p-1}{2}},$$

poniendo en vez de los productos D, $2D$..... sus restos respectivos, la que sigue:

$$a_1\, a_2 \ldots\ldots a_\mu \,.\, b_1\, b_2 \ldots\ldots b_\lambda \equiv 1 \,.\, 2 \,.\, 3 \ldots\ldots \tfrac{1}{2}(p-1)D^{\frac{p-1}{2}} \pmod{p},$$

Mediante esta congruencia, se convierte la de arriba en la siguiente:

$$(-1)^\mu \,.\, 1 \,.\, 2 \,.\, 3 \ldots\ldots \tfrac{1}{2}(p-1) \,.\, D^{\frac{p-1}{2}} \equiv 1 \,.\, 2 \,.\, 3 \ldots\ldots \tfrac{1}{2}(p-1) \pmod{p},$$

ó bien, suprimiendo el producto comun á los dos miembros, en esta otra:

$$(-1)^\mu \,.\, D^{\frac{p-1}{2}} \equiv 1 \pmod{p}:$$

de la cual se deduce:

$$D^{\frac{p-1}{2}} \equiv (-1)^\mu \pmod{p},$$

ó, en otros signos:

$$\left(\frac{D}{p}\right) = (-1)^\mu.$$

Esta expresion simbólica traducida al lenguaje vulgar dice así:
Un número cualquiera D, primo con p, será resto, ó no-resto cua-

drático de p, *segun que el número* μ, *de los restos mínimos positivos* (mod. p), *mayores que* $\frac{1}{2}p$, *de los productos*

$$D,\ 2D,\ 3D,\ \ldots\ldots\ \tfrac{1}{2}(p-1)D,$$

sea par, ó impar.

Ejemplo 1.° *Nos proponemos averiguar si* $3 = D$ *es resto ó no-resto del módulo* $17 = p$. Formando los productos de 3 por los $\frac{1}{2}(17-1) = 8$ primeros números enteros, tendremos:

$$3,\quad 6,\quad 9,\quad 12,\quad 15,\quad 18,\quad 21,\quad 24,$$

cuyos restos, segun 17, son respectivamente

$$3,\quad 6,\quad 9,\quad 12,\quad 15,\quad 1,\quad 4,\quad 7:$$

y, como entre estos restos hay *tres* $= \mu$ á saber;

$$9,\quad 12,\quad 15,$$

que son mayores que $\frac{1}{2}p = 8\frac{1}{2}$, resulta que 3 es no-resto de 17.

Ejemplo 2.° *Veamos si* 8 *es resto ó no-resto del mismo* 17.

Los productos de 8 por los ocho primeros números son:

$$8,\quad 16,\quad 24,\quad 32,\quad 40,\quad 48,\quad 56,\quad 64,$$

y sus restos mínimos positivos, segun 17,

$$8,\quad 16,\quad 7,\quad 15,\quad 6,\quad 14,\quad 5,\quad 13;$$

entre los cuales hay *cuatro* $= \mu$, 16, 15, 14, 13, que son mayores que $\frac{1}{2}p = 8\frac{1}{2}$: luego 8 es resto de 17.

Hé aquí una tabla que contiene algunos números primos y sus restos cuadráticos correspondientes:

Números.	*Restos cuadráticos.*	*Su conjunto.*
3	1	1
5	1, 4	2
7	1, 2, 4	3
11	1, 3, 4, 5, 9	5
13	1, 3, 4, 9, 10, 12	6
17	1, 2, 4, 8, 9, 13, 15, 16	8
19	1, 4, 5, 6, 7, 9, 11, 16, 17	9
23	1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18	11
29	1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28	14
31	1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28	15
37	1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36	18

En esta tabla se ve perfectamente que el número de restos, para cada módulo p, es, en efecto, $\frac{1}{2}(p-1)$; en cambio los otros números del sistema de restos de p que no figuran en ella, son no-restos de los módulos respectivos. Así, v. gr.: 2 es no-resto de 3; 2 y 3 no-restos de 5, etc.

Explicada la teoría de los restos cuadráticos, para un número primo, fundándonos exclusivamente en las propiedades de los números socios y en las elementales (63) de los restos que producen los productos sucesivos de un número no divisible por el módulo, pasemos ahora á confirmar lo dicho, y completar aquella respecto del módulo 2, y de los módulos compuestos, apoyándonos tambien en los principios generales que al tratar de las congruencias binomias expusimos.

106.—*De la congruencia* $x^2 \equiv D \pmod{p}$, *cuando* p *sea un número primo impar.*

Aplicando dichos principios (98) al caso actual, tenemos: $n = 2$, y $\delta = 2 =$ máximo comun divisor del grado 2 y de $p - 1$ que es par; de cuyos datos se desprende que la congruencia

$$x^2 \equiv D \pmod{p} \qquad (1)$$

será posible siempre que se verifique la condicional

$$D^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \qquad (2$$

y entónces, para cada número D, admitirá dos raices incongruentes.

De esta congruencia y del teorema de Fermat

$$D^{p-1} - 1 = \left(D^{\frac{p-1}{2}} - 1 \right) \left(D^{\frac{p-1}{2}} + 1 \right) \equiv 0 \pmod{p},$$

se deduce que D, cuando sea no-resto cuadrático de p, debe satisfacer á esta otra:

$$D^{\frac{p-1}{2}} = -1 \pmod{p}.$$

que con la anterior expresa el carácter de *Euler*.

Ambas prueban que el conjunto de los números D, ó el número de los *restos* cuadráticos de p, es igual, al de los *no-restos* de dicho módulo, esto es, $= \frac{1}{2}(p-1)$; y de ellas se desprende además que, si g es una raiz primitiva de p, las potencias pares de g,

$$g^0, \; g^2, \; g^4, \; \ldots\ldots \; g^{p-3},$$

representan los restos de p, y las impares, $g^1, g^3, g^5, \ldots\ldots g^{p-2}$, los no-restos.

De lo cual se infiere tambien que los restos cuadráticos de p no son raices primitivas de p; porque pertenecen al exponente $\frac{1}{2}(p-1)$, que es menor que $p-1=\varphi(p)$; y, de consiguiente, las raices primitivas de p se encontrarán entre los *no-restos* del mencionado número p; ó son además no-restos de p.

Resulta, finalmente, que por el procedimiento seguido ahora hemos llegado á determinar, como por el directo y elemental, seguido antes, cuáles y cuántos son los restos cuadráticos del módulo primo, impar, p, y cuántas raices admite la congruencia $x^2 \equiv D \pmod{p}$ para cada uno de aquellos restos.

107.—*De la congruencia* $x^2 \equiv D \pmod{k}$, *cuando* k *sea una potencia cualquiera de un número primo impar.*

Supongamos $k=p^\pi$, y que la congruencia

$$x^2 \equiv D \left(\text{mod. } p^\pi\right) \qquad (1)$$

sea posible; entónces, decimos, esta congruencia admitirá dos raices incongruentes. En efecto, sea α una de ellas, que verificará naturalmente la congruencia

$$\alpha^2 \equiv D \left(\text{mod. } p^\pi\right). \qquad (2)$$

Restando ésta de la anterior, se obtiene la diferencia

$$x^2 - \alpha^2 = (x+\alpha)(x-\alpha) \equiv 0 \left(\text{mod. } p^\pi\right).$$

Ahora bien, de los dos factores binomios de esta diferencia, uno solo puede ser divisible por p; porque, si lo fueran los dos á un tiem-

po, su diferencia $(x+\alpha)-(x-\alpha)=2\alpha$ lo sería tambien; y, como 2 es primo con p, deberia ser α múltiplo de p; y, por consecuencia, segun la congruencia (2), tambien D divisible por p: lo cual es contra la hipótesis que desde un principio sentamos, de ser D primo con p. Esto prueba que uno solo de los dos factores expresados, indistintamente, ha de ser divisible por p^{π}; y, de la suposicion de que lo sea el segundo, ó el primero, resultan las congruencias

$$x \equiv \alpha \left(\text{mod. } p^{\pi}\right), \quad \text{ó} \quad x \equiv -\alpha \left(\text{mod. } p^{\pi}\right);$$

las cuales patentizan que la propuesta (1) admite las dos raices α y $-\alpha$, ó no admite ninguna.

Segun los principios generales (101), la congruencia (1) será resoluble cuando se verifique la condicional

$$D^{\frac{1}{2}\varphi\left(p^{\pi}\right)} \equiv 1 \left(\text{mod. } p^{\pi}\right);$$

pero se puede tambien reducir al anterior el caso presente, esto es, deducir la posibilidad de la congruencia dada ahora,

$$x^2 \equiv D \left(\text{mod } p^{\pi}\right), \qquad (1)$$

de la posibilidad de la anteriormente considerada,

$$x^2 \equiv D \left(\text{mod. } p\right). \qquad (2)$$

Que toda raiz α de la congruencia (1) lo es tambien de la congruencia (2) es evidente, y no hay para qué insistir en ello. Mas lo importante es saber si, recíprocamente, de una raiz α de la congruencia (2), segun la primera potencia de p, se puede deducir otra, congruente ó equivalente á aquella (mod. p), que satisfaga á la congruencia (1), segun una potencia cualquiera de p; y para esto es claro que

basta indagar si de una raiz α de la congruencia (1) puede deducirse otra $\equiv \alpha \pmod{p^\pi}$ que verifique la congruencia

$$x^2 \equiv D \pmod{p^{\pi+1}}. \qquad (3)$$

Fácil es y muy breve la investigacion indicada. En efecto, si α es raiz de la congruencia (1) tendremos:

$$\alpha^2 \equiv D \pmod{p^\pi} \quad \text{ó bien} \quad \alpha^2 - D = hp^\pi,$$

siendo h entero. Estableciendo la igualdad

$$x = \alpha + p^\pi y,$$

elevándola al cuadrado, restando D luego de los dos miembros, y teniendo presente el valor de $-D$, resulta:

$$x^2 - D = hp^\pi + 2\alpha p^\pi y + p^{2\pi} y^2 \equiv p^\pi (h + 2\alpha y) \pmod{p^{\pi+1}};$$

y de aquí que, si ha de ser $x^2 - D$ divisible por $p^{\pi+1}$, ó lo que es igual,

$$x^2 \equiv D \pmod{p^{\pi+1}},$$

es necesario que $h + 2\alpha y$ sea divisible por p, ó bien que

$$2\alpha y \equiv -h \pmod{p}.$$

En esta última congruencia, 2α es conocido, y h está determinado por la igualdad $h = (\alpha^2 - D) : p^\pi$; de modo que, si la variable y puede tambien determinarse para que aquella se verifique, quedará demostrado lo que pretendíamos. Mas en esta congruencia de primer grado que contiene la y, como D, y, por lo tanto, α, son primos con p, y, por ser p impar, tampoco 2α es divisible por p, el coeficiente

2α, de la incógnita y, es primo con el módulo: luego siempre (68) será posible determinar y mediante la congruencia expresada; y, por consecuencia, deducir de una raiz α de la (1) otra de la congruencia (3). Nótese además, que no solamente hemos demostrado que la posibilidad de la congruencia (1) lleva consigo la de la (3); y, repitiendo el mismo razonamiento, que de una raiz de la congruencia cuyo módulo sea la primera potencia de p, puede deducirse otra de la congruencia cuyo módulo sea el cuadrado de p; de ésta una tercera cuyo módulo sea el cubo de p, etc.; sino que en la misma demostracion se halla indicado el medio práctico de encontrar estas raices.

Veamos, por ejemplo, cómo, dada la congruencia

$$x^2 \equiv 7 \pmod{3}, \qquad (1)$$

y una raiz de la misma $\alpha = 1$, se hallará otra raiz de la congruencia

$$x^2 \equiv 7 \pmod{3^4}. \qquad (2)$$

Siendo $\alpha = 1$ una raiz de la congruencia (1), tenemos:

$$1 \equiv 7 \pmod{3};$$

de donde se deduce:

$$h = \frac{1-7}{3} = -2; \quad \text{y, por lo tanto,} \quad 2y \equiv +2 \pmod{3}; \; y \equiv 1.$$

Sustituyendo este valor de y en la expresion

$$x = \alpha + py,$$

se obtiene el de $\alpha' = 1 + 3 = 4$ para raiz de la congruencia

$$x^2 \equiv 7 \pmod{3^2},$$

Con los datos referentes á esta congruencia $\alpha' = 4$, $D = 7$, $p^{\pi} = 9$, se hallan:

$$h = \frac{4^2 - 7}{9} = 1;\ 2y' \equiv -1 \pmod{3};\ y' = 1;\ \alpha'' = 4 + 9 = 13.$$

Siendo $\alpha'' = 13$ una raiz de la congruencia

$$x^2 \equiv 7 \pmod{3^3},$$

como en los casos anteriores tendremos:

$$h = \frac{13^2 - 7}{27} = \frac{169 - 7}{27} = 6;\ 2y'' \equiv -6 \pmod{31};\ y'' = 0;$$

$$\alpha''' = 13 + 0 = 13.$$

Así vemos efectivamente que á la raiz $\alpha = 1$ de la congruencia (1) corresponde la $\alpha''' = 13 \equiv \alpha \pmod{3}$ de la congruencia (2); y, si en lugar de la raiz 1 hubiésemos tomado la otra $\alpha = -1$, hubiéramos hallado del mismo modo, $\alpha''' = -13$.

108.—*De la congruencia* $x^2 \equiv D \pmod{k}$, *cuando* k *sea una potencia superior á la primera del número* 2.

Ante todo advertiremos acerca del caso excluido en este epígrafe, de ser el módulo igual á 2, que todo número impar es congruente con $1^2 \pmod{2}$, y, por consecuencia, resto cuadrático de 2.

La congruencia referente á la segunda potencia de 2,

$$x^2 \equiv D \pmod{4},$$

será posible siempre que se verifique la condicional

$$D \equiv 1 \pmod 4;$$

porque, admitida su posibilidad, cualquiera raiz x que la satisfaga, tiene que ser un número impar, de la forma $2n+1$ por ejemplo, cuyo cuadrado, $4n^2+4n+1$, es en efecto $\equiv 1 \pmod 4$; y recíprocamente: si se verifica la condicional $D \equiv 1 \pmod 4$, la congruencia $x^2 \equiv 1 \pmod 4$ contiene evidentemente las dos raices $x \equiv \pm 1 \pmod 4$.

La congruencia, segun la tercera potencia de 2,

$$x^2 \equiv D \pmod 8,$$

será posible cuando se verifique la condicional

$$D \equiv 1 \pmod 8;$$

puesto que el cuadrado de todo número impar $4n \pm 1$, es

$$16n^2 \pm 8n + 1 \equiv 1 \pmod 8;$$

y, recíprocamente: si esta condicion se cumple, la congruencia propuesta, entónces convertida en esta otra, $x^2 \equiv 1 \pmod 8$, contiene las cuatro raices $x \equiv 1$, $x \equiv 3$, $x \equiv 5$, $x \equiv 7$.

Pasemos ya á la congruencia más general

$$x^2 \equiv D \left(\text{mod. } 2^\lambda\right), \qquad (1)$$

en la cual sea $\lambda \geqslant 3$. Esta congruencia será posible cuando se verifique la condicional

$$x^2 \equiv D \pmod 8,$$

y para esto es necesario que

$$D \equiv 1 \pmod 8. \qquad (2)$$

Pero tambien recíprocamente: si esta condicion se cumple, la congruencia general propuesta es posible, y admite cuatro raices incongruentes $(\text{mod. } 2^{\lambda})$. Para demostrar lo primero, siguiendo el mismo método inductivo que en el párrafo anterior, admitamos que sea α una raiz de la congruencia (1), en cuyo supuesto será

$$\alpha^2 - D = h \cdot 2^{\lambda}.$$

Estableciendo la igualdad

$$x = \alpha + 2^{\lambda-1} \cdot y,$$

elevándola al cuadrado, restando luego D de sus dos miembros, y cambiando $\alpha^2 - D$ por su valor $h \cdot 2^{\lambda}$, tendremos la siguiente:

$$x^2 - D = h \cdot 2^{\lambda} + 2^{\lambda} \cdot \alpha y + 2^{2\lambda-2} \cdot y^2;$$

ó, reparando en que $2\lambda - 2$ es $\geqq \lambda + 1$ por ser $\lambda \geqq 3$, la congruencia:

$$x^2 - D \equiv 2^{\lambda}(h + \alpha y) \, (\text{mod. } 2^{\lambda+1}).$$

Ahora bien, para que $x^2 - D$ sea divisible por $2^{\lambda+1}$, ó, en otros términos, para que x sea raiz de la congruencia

$$x^2 \equiv D \, (\text{mod. } 2^{\lambda+1}), \qquad (3)$$

es necesario y suficiente que $h + \alpha y$ sea divisible por 2; y, como siempre es posible (68) determinar y mediante la congruencia

$$\alpha y \equiv -h \, (\text{mod. } 2),$$

por ser α impar, y, de consiguiente, primo con 2, resulta que la posibilidad ó existencia de una raiz α para la congruencia (1), exije inevitablemente la posibilidad de la congruencia (3); y, por conclusion, que:

Para ser posible la congruencia

$$x^2 \equiv D \pmod{2^\lambda}$$

es necesario y suficiente que se cumpla la condicion

$$D \equiv 1 \pmod{8}.$$

Para lo segundo, representemos, como antes, por α una raiz de la congruencia (1), será evidentemente:

$$x^2 - \alpha^2 = (x-\alpha)(x+\alpha) \equiv 0 \pmod{2^\lambda};$$

y, dividiendo por 2^2 sus dos miembros y el módulo, lo cual es posible por ser x y α impares, esta otra:

$$\frac{x-\alpha}{2} \cdot \frac{x+\alpha}{2} \equiv 0 \pmod{2^{\lambda-2}};$$

mas la diferencia

$$\frac{x+\alpha}{2} - \frac{x-\alpha}{2} = \alpha.$$

es un número impar, α; y para esto es indispensable que uno de sus dos términos, ó factores de la última congruencia, $\frac{1}{2}(x-\alpha)$ ó $\frac{1}{2}(x+\alpha)$, indistintamente sea impar, y el otro, como exije esta misma, divisible por $2^{\lambda-2}$; luego por precision habrá de verificarse una de las siguientes:

$$x \equiv \alpha \pmod{2^{\lambda-1}}, \quad \text{ó} \quad x \equiv -\alpha \pmod{2^{\lambda-1}}.$$

Estas congruencias manifiestan que la suma ó la diferencia de los números, α y x, es divisible por $2^{\lambda-1}$: lo cual exije que, si uno

de ellos es α, el otro x tenga la forma, ya establecida, $\alpha + 2^{\lambda-1}.y$, cuyo cuadrado es $\equiv \alpha^2 \equiv D \pmod{2^\lambda}$; y de las mismas se desprenden, por consecuencia, los cuatro valores de x que á continuacion figuran:

$$x \equiv \alpha \pmod{2^\lambda} \qquad x \equiv \alpha + 2^{\lambda-1} \pmod{2^\lambda}$$

$$x \equiv -\alpha \pmod{2^\lambda} \qquad x \equiv -\alpha - 2^{\lambda-1} \pmod{2^\lambda},$$

Que estos cuatro valores incongruentes $\pmod{2^\lambda}$ de la variable x satisfacen á la congruencia propuesta no hay para qué repetirlo despues de lo dicho.

En resumen:

La congruencia

$$a^2 \equiv D \pmod{2^\lambda},$$

será posible:

1.° *Cuando* $\lambda = 1$, *siempre; y entónces admite una sola raiz.*

2.° *Cuando* $\lambda = 2$, *siempre que se cumpla la condicion* $D \equiv 1 \pmod{4}$; *y entónces admite dos raices.*

3.° *Cuando* $\lambda \geq 3$, *siempre que se cumpla la condicion* $D \equiv 1 \pmod{8}$; *y entónces admite cuatro raices.*

109.—*De la congruencia* $x^2 \equiv D \pmod{k}$ *cuando* k *sea un número cualquiera.*

Esta congruencia, en la cual se supone siempre D primo con k, será posible cuando lo sean las congruencias correspondientes á cada uno de los factores primos de su módulo; y, como este módulo sólo puede contener factores primos impares, potencias de estos números primos, y el número primo 2 ó sus potencias superiores, ya exclusivamente una sola especie de estos factores, bien mezclados unos con otros,

en los párrafos precedentes queda explicado cuanto para la resolucion del caso actual necesitamos.

Supongamos, pues, que k no contenga el factor 2, por el pronto, y designemos por p un factor cualquiera, primo, de k; la congruencia

$$x^2 \equiv D \,(\text{mod. } k) \qquad (1)$$

será posible siempre que se verifique la condicional, referente á los factores p,

$$\left(\frac{D}{p}\right) = +1; \qquad (2)$$

y, entónces, para cada uno de los factores de la forma p^π, de su módulo k, admitirá *dos* raices incongruentes; luego, si μ representa el número de todos estos factores primos diferentes, p, el de las raices incongruentes de la congruencia propuesta (1), será

$$\sigma = 2^\mu.$$

Supongamos ahora que k contenga el factor 2; tendremos que distinguir tres casos: que contenga simplemente á dicho factor; que le contenga elevado á la segunda potencia; ó á una potencia igual ó superior á la tercera.

En el primero será k el duplo de un número impar, y como la congruencia para el módulo 2,

$$x^2 \equiv D \,(\text{mod. } 2)$$

admite una sola raiz, la propuesta (1) admitirá el mismo número σ de raices que cuando no contenia su módulo al factor 2.

En el segundo, será k el cuádruplo de un número impar, y á la condicion general (2), referente á los factores impares, habrá que añadir esta otra,

$$D \equiv 1 \,(\text{mod. } 4),$$

para que sea posible la congruencia (1); la cual, como la correspondiente al módulo 4 admite *dos* raices, admitirá entónces

$$\sigma = 2^{\mu}.2 = 2^{\mu+1}.$$

En el tercero, será k el óctuplo de un número impar; á la condicion general (2) habrá que añadir esta otra:

$$D \equiv 1 \pmod{8};$$

y, como la congruencia

$$x^2 \equiv D \left(\text{mod. } 2^{\lambda}\right),$$

donde $\lambda \geq 3$, admite, cuando es posible se entiende, *cuatro* raices incongruentes, la propuesta (1) admitirá para este caso

$$\sigma = 2^{\mu}.4 = 2^{\mu+2}.$$

Con esto la primera parte de la teoría de los restos cuadráticos (103) queda por completo terminada; mas, ántes de pasar á la segunda, conviene tratar en seguida, como consecuencia de los principios que acabamos de estudiar, de la generalizacion del teorema Wilson, ya exclusivamente para los números primos demostrado.

110.—*Teorema de Wilson generalizado.*

Haciendo $D = 1$ en la congruencia (1) del párrafo anterior, la resultante

$$x^2 \equiv 1 \pmod{k} \qquad (1)$$

es siempre posible, y el número σ de sus raices es: 1, cuando $k = 1$, ó $k = 2$; 2, cuando k es una potencia cualquiera de un número primo impar, el duplo de tal potencia, ó igual á 4; ó múltiplo de 4, en

todos los demás casos. Omitiendo los dos primeros, $k = 1$, y $k = 2$, para los cuales es $\sigma = 1$, este número σ puede distribuirse en $\frac{1}{2}\sigma$ pares de raices, tales como ρ y $-\rho$, las cuales son incóngruas ó diferentes entre sí (mod. k), por ser ρ primo con k, y, de consiguiente, su diferencia 2ρ no divisible por k. El producto de este par de raices, $\rho \times (-\rho) = -\rho^2$, es $\equiv -1$; y, por consecuencia, segun que σ contenga, ó no, un número par de estas parejas, esto es, segun que σ sea, ó no, divisible por 4, así el producto de todas las σ raices de la congruencia (1) será $\equiv +1$ ó $\equiv -1$; y, en general, será $\equiv (-1)^{\mu}$, si μ representa el número de las parejas mencionadas, ρ y $-\rho$. Pero estas σ raices se encuentran entre los $\varphi(k)$ números primos con k é inferiores á este número; y quitándolas de ellos, los restantes $\varphi(k) - \sigma$, si quedan, pueden tambien agruparse en parejas (*) de sócios (r, s) (88) cuyo producto $rs \equiv 1$, segun sabemos, y los cuales son tambien diferentes entre sí; pues, si fuesen congruentes, $s \equiv r$, tendríamos $r^2 \equiv 1$, y sería r, por lo tanto, una de las σ raices de la congruencia (1). Luego el producto de todos los $\varphi(k)$ números inferiores y primos con k es $\equiv +1$ ó $\equiv -1$, segun que σ sea, ó no, divisible por 4; ó bien, segun que μ sea par ó impar; y, por consecuencia:

Si P representa el producto de los $\varphi(k)$ números primos con k é inferiores á este número, se verificará la congruencia

$$P \equiv \mp 1 \pmod{k}:$$

á saber:

$$P \equiv -1 \pmod{k},$$

siempre que sea $k =$ una potencia cualquiera de un número primo impar, el duplo de tal potencia, ó $= 4$; y

$$P \equiv +1 \pmod{k}$$

en todos los demás casos.

(*) El número $\varphi(k)$ es siempre par, excepto en los casos $k = 1$, $k = 2$ (55).

En cuanto á los en un principio exceptuados, $k = 1$, $k = 2$, siempre es $\varphi(k) = 1$, y el único número no mayor y primo con k, de consiguiente, $\equiv \pm 1$.

Tal es el teorema que lleva el nombre de *teorema generalizado de Wilson.*

Segunda parte.—111.—*Verdadero concepto del asunto.*

Pasemos ya á estudiar la segunda parte (103) de la teoría de los restos cuadráticos, á saber:

Hallar todos los módulos k de los cuales un número conocido D sea resto cuadrático.

Para ésto comencemos por enunciar en términos bien esplícitos la índole y extension del problema que tratamos de resolver.

En general, los *módulos* k, para los cuales se verifica la congruencia $f(x) \equiv 0 \pmod{k}$, se llaman tambien *divisores de la forma* $f(x)$, dado que existan, por supuesto, números x, que hagan esta forma divisible por alguno de aquellos módulos. Aplicando esta definicion á la congruencia particular

$$x^2 \equiv D \pmod{k}, \quad \text{ó} \quad x^2 - D \equiv 0 \pmod{k},$$

diremos que los módulos k, de cuya determinacion tratamos ahora, son los divisores de la forma

$$x^2 - D. \tag{1}$$

Pero los divisores de esta forma lo son tambien de la forma más general

$$t^2 - Du^2 \tag{2}$$

en la cual representan t, u dos números enteros indeterminados, y siempre primos entre sí, puesto que la última forma se convierte en la

primera con solo hacer $t = x$, $u = 1$. Y recíprocamente: todo divisor de la forma (2), en la cual t, u expresan números primos relativos, es tambien divisor de la forma (1); porque designando k un divisor de la (2), este divisor sería primo con u (en atencion á que cualquier factor comun de k y u lo sería tambien de t, y entónces t y u no serian primos entre sí), y podríamos hallar siempre (68) un número x que verificase la congruencia $ux \equiv t \pmod{k}$. Elevando, pues, al cuadrado esta congruencia posible, y sumándola luego con la supuesta (2),

$$t^2 - Du^2 \equiv 0 \pmod{k},$$

resultará la siguiente:

$$u^2(x^2 - D) \equiv 0 \pmod{k},$$

ó bien, como u es primo con k, esta otra (61-8.ª),

$$x^2 - D \equiv 0 \pmod{k}.$$

Luego la posibilidad de una de las dos congruencias

$$x^2 - D \equiv 0, \qquad t^2 - Du^2 \equiv 0 \pmod{k},$$

lleva consigo la de la otra: y, por consecuencia, el problema poco ántes enunciado, podrá tambien formularse en estos otros términos:

Hallar todos los divisores de la forma $t^2 - Du^2$, *en la cual* D *representa un número dado, y* t, u *dos indeterminados, sujetos á la condicion de ser primos entre sí.*

Concretándonos tambien en esta parte de la cuestion, como en la primera, á los módulos k (siempre positivamente considerados) primos con D, y recordando que la posibilidad de la congruencia

$$x^2 \equiv D \pmod{k},$$

depende exclusivamente de las propiedades de los factores primos impares contenidos en k, y que la misma congruencia es muy fácil de resolver para los módulos de la forma 2^{λ}, podremos reducir nuestro problema á determinar los módulos primos impares p, primos con D, de los cuales sea este número conocido, D, resto cuadrático. Como por otra parte, el carácter del número D, respecto de tales módulos, depende tambien de sus factores, y este número D en general, y á condicion de ser primo con un módulo primo impar p, puede ser positivo ó negativo, par ó impar, el problema planteado se concreta en último término al siguiente:

Hallar los números primos impares, p, para los cuales sea posible una de las tres congruencias

$$x^2 \equiv -1, \quad x^2 \equiv 2, \quad x^2 \equiv q \pmod{p},$$

designando q tambien un número primo impar, positivo y dado.

O, usando la notacion de Legendre, á

Determinar el valor de los tres símbolos:

$$\left(\frac{-1}{p}\right), \left(\frac{2}{p}\right), \left(\frac{q}{p}\right).$$

112.—*Determinacion del símbolo* $\left(\frac{-1}{p}\right)$.

La determinacion de las formas de los módulos p que satisfagan á la congruencia

$$x^2 \equiv -1 \pmod{p},$$

no ofrece dificultad ninguna. En efecto, aplicando el criterio general de Euler y Legendre,

$$\left(\frac{D}{p}\right) \equiv D^{\frac{p-1}{2}} \pmod{p},$$

al valor particular de $D = -1$, tendremos:

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p},$$

ó si se quiere mejor:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Esta igualdad manifiesta que el símbolo de su primer miembro será la unidad positiva ó negativa, segun que el exponente $\frac{1}{2}(p-1)$ del segundo, sea par ó impar. Ahora bien, todos los números primos impares, al ser divididos por 4, producen los restos 1 ó 3; y de aquí se desprende que todos aquellos números primos se dividen en dos clases, respecto del módulo 4, cuyas formas respectivas son $4n+1$ y $4n+3$: si p es de la primera, el exponente $\frac{1}{2}(p-1)$ es par, y, por consecuencia, -1 resto cuadrático de p; si fuese de la segunda, $\frac{1}{2}(p-1)$ sería impar, y -1, por lo tanto, no-resto entónces de p. Luego

El número -1 *es resto cuadrático de todos los números primos de la forma* $4n+1$, *y no-resto de todos los números primos de la forma* $4n+3$.

Al mismo resultado puede llegarse por este otro camino.

Elevando la congruencia, supuesta posible,

$$x^2 \equiv -1 \pmod{p},$$

á la potencia $\frac{1}{2}(p-1)$, se obtiene la siguiente:

$$x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p},$$

y, segun el teorema de Fermat,

$$1 \equiv (-1)^{\frac{p-1}{2}} \pmod{p};$$

para lo cual es necesario que p sea de la forma $4n+1$; y, por consecuencia, -1 es no-resto cuadrático de los números primos de la forma $4n+3$.

Recíprocamente, si p es de la forma $4n+1$, el binomio de Fermat, $x^{p-1}-1$, es divisible algebráicamente por $x^4-1=(x^2+1)(x^2-1)$, y, por lo tanto, por x^2+1: luego será

$$x^{p-1}-1=(x^2+1)\psi(x),$$

donde $\psi(x)$ representa un polinomio con coeficientes enteros; de cuya igualdad (80) se deduce que la congruencia $x^2 \equiv -1$, ó mejor el binomio x^2+1 será congruente con cero para dos valores incongruentes de x; y, de consiguiente que el número -1 es resto cuadrático de todos los números primos de la forma $4n+1$.

Este resultado se obtiene tambien muy fácilmente, supuesto el teorema de Wilson. En efecto, entre los números $1, 2, 3, \ldots\ldots (p-1)$, sabemos que existen $\frac{1}{2}(p-1)$ restos, y otros tantos no-restos de p; y, por consecuencia, el número de los no-restos de p será par, ó impar, segun que dicho módulo sea de la forma $4n+1$, ó de la forma $4n+3$; siendo así, en el primer caso, resto, y en el segundo, no-resto de p, el producto $1.\ 2.\ 3.\ \ldots\ldots (p-1)$ de los restos de p; mas este producto, segun el teorema mencionado, es siempre $\equiv -1$; luego -1 será tambien resto de $p=4n+1$, y no-resto de $p=4n+3$.

Infiérese además de lo anterior que, si r es *resto* de un número primo de la forma $4n+1$, será tambien $-r$ *resto* de este número; y todos los *no-restos* del mismo permanecerán *no-restos* aunque cambien

de signo; pero, si fuese p de la forma $4n+3$, sus *restos* se convertirán en *no-restos* al cambiar de signo, y vice-versa.

113.—*Determinacion del símbolo* $\left(\frac{2}{p}\right)$.

El número 2 *es resto cuadrático de todos los números primos de las formas* $8n \pm 1$, *y no-resto de todos los números primos de las formas* $8n \pm 3$.

Aplicando los principios generales (104), sustituiríamos en la congruencia condicional

$$2^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

en lugar de p, las cuatro formas espresadas (*):

$$8n+1, \quad 8n-1, \quad 8n+3, \quad 8n-3,$$

y discutiríamos en qué casos era su primer miembro $\equiv +1$, y en cuales $\equiv -1$; pero creemos más conveniente, conforme nos enseña Gauss (**), demostrar esta proposicion por el método inductivo.

En la tabla de restos cuadráticos (105) vemos efectivamente que el número 2 es resto de los números

$$7, \quad 17, \quad 23, \quad 31, \quad 41, \quad \ldots\ldots$$

entre los cuales ninguno hay de las formas $8n+3$ y $8n-3 = 8n+5$. Prolongando la tabla hasta el número 100, por ejemplo, veríamos el mismo resultado: que ningun número primo, menor que 100, del cual

(*) Skrivan, Grundlehren der Zahlen-Theorie, §. 84.
(**) D. A., §§. 112 y 113.

fuese 2 resto cuadrático, tendría la forma $8n+3$, ni la forma $8n+5$; y, si probáramos, en general, que esta induccion es cierta, podríamos afirmar que no existe ningun número primo de las formas $8n+3$ y $8n+5$, cuyo resto cuadrático sea 2. Supongamos para esto que, pasado cierto límite, existan números de las formas $8n\pm3$, de los cuales sea 2 resto cuadrático; y designemos por p el *mínimo* de todos ellos; de manera que p será de una de las formas $8n+3$ ú $8n+5$, y el número 2 resto cuadrático de p, pero no-resto de todos los números, menores que p, cuyas formas sean tambien $8n+3$ ú $8n+5$. Siendo 2 resto de p, la congruencia

$$x^2 \equiv 2 \text{ (mod. } p),$$

será posible y admitirá, como sabemos, dos raices, a y $a'=p-a$, cuya suma es p, ambas menores que p, por consecuencia, y par la una, é impar la otra. Sea, pues, a la raiz impar y menor que p, que verifica la congruencia

$$a^2 \equiv 2 \text{ (mod. } p), \qquad (1)$$

Escribiendo esta congruencia en forma de ecuacion tendremos:

$$a^2 - 2 = pf; \qquad (2)$$

de la cual, como a es impar, y a^2, por lo tanto, de la forma $8n+1$, se desprende que el producto $pf=a^2-2$ es de la forma $8n-1$; y para que este producto sea de la forma expresada, $8n-1$, siendo uno de sus factores p, que tiene las formas $8n\pm3$, es necesario que el otro factor f sea de las formas respectivamente $8n\mp3$. Por consecuencia, todos los factores primos que puede contener f, afectarán, respecto del módulo 8, exclusivamente las cuatro formas $8n\pm3$, $8n\pm1$; y, puesto que el producto de los números de las dos últimas es tambien de estas mismas formas, $8n\pm1$, síguese que el número f por precision ha de contener un factor primo p', aunque él lo sea, de una de las dos primeras $8n\pm3$. Pero de la igualdad (2) se deduce que la

congruencia (1) se verifica tambien para el módulo f, y, de consiguiente, para el divisor p' de este módulo, esto es:

$$a^2 \equiv 2 \pmod{p'};$$

y, como p' es menor que p, resulta, contra la hipótesis en el principio admitida, que p no es el *mínimo* número de las formas $8n \pm 3$, del cual sea 2 resto cuadrático: luego tal hipótesis debe desecharse, y establecerse en general:

$$\left(\frac{2}{p}\right) = -1, \quad \textit{cuando} \quad p = 8n \pm 3.$$

Para demostrar ahora que el número 2 es resto cuadrático de todos los números de la forma $8n+7 = 8h-1$, como $2 = -1 \times -2$, y -1 es no-resto de la forma $4n-1$, equivalente á la anterior, bastaría demostrar que -2 es no-resto tambien de esta misma forma; pues el producto de dos no-restos (104) es un resto. Pero vamos á tratar la cuestion más ámpliamente, probando á un tiempo que el número -2 es no-resto de los números primos, contenidos en las dos formas $8n+5$ y $8n+7$, aunque para los de la primera $8n+5 = 4h+1$, de los cuales es -1 resto, ya queda más arriba demostrado.

Desde luego vemos que la ley enunciada es cierta para el número 5, mínimo de los contenidos en una de las dos formas propuestas; pero supongamos que no sea cierta, en general, y que p represente el *primero* de los números de dichas formas, contando de menor á mayor, para el cual sea -2 resto cuadrático. Entónces, tomando, como antes, la raiz a, impar y menor que p, de la congruencia

$$a^2 \equiv -2 \pmod{p},$$

el número f, contenido en la igualdad consiguiente,

$$a^2 + 2 = pf,$$

será tambien aquí positivo, impar y menor que p; a^2 será de la forma $8n+1$, y, por consecuencia, a^2+2, ó pf, de la forma $8n+3$; y

para esto es necesario que, si p tiene la forma $8n+5$, tenga f la forma $8n+7$; y, si p es de la forma $8n+7$, sea f de la $8n+5$. Ahora bien, como un producto de factores exclusivamente de la forma $8n+1$, ó de la $8n+3$, es siempre de la primera ó de la segunda de estas formas tambien, y no puede afectar jamás las formas $8n+5$ ni $8n+7$, resulta que el número f, que tiene una de estas últimas, necesariamente habrá de contener algun factor primo, p', de alguna de ellas, el cual verificará la congruencia

$$x^2 \equiv -2 \text{ (mod. } p'\text{)}:$$

de donde se concluye que -2 es resto tambien del número $p' < p$; y, por consecuencia, que la suposicion que hicimos de ser p el *mínimo*, para el cual dejaba de ser -2 no-resto y se convertia en resto, es inadmisible, pudiéndose establecer en general la ecuacion:

$$\left(\frac{-2}{p}\right) = -1, \text{ } \textit{cuando} \text{ } p = 8n+5 \text{ ú } 8n+7;$$

y, teniendo en cuenta que -1 es resto de $8n+5$, y no-resto de $8n+7$, estas otras:

$$\left(\frac{2}{p}\right) = -1, \text{ } \textit{cuando} \text{ } p = 8n+5.$$

$$\left(\frac{2}{p}\right) = +1, \text{ } \textit{cuando} \text{ } p = 8n+7.$$

Nos falta considerar todavía la forma $8n+1$, ó lo que es igual, demostrar que el número 2 es resto de los números primos de esta forma. El método inductivo en los casos anteriores empleado no es aplicable en éste; pero muy sencillamente puede suplirse como sigue:

Siendo p de la forma $8n+1$, el binomio de Fermat

$$x^{p-1} - 1,$$

contiene al divisor $x^8 - 1 = (x^4 - 1)(x^4 + 1)$, y, por lo tanto, al factor $x^4 + 1$; de donde se deduce (80) que la congruencia

$$x^4 + 1 \equiv 0 \,(\text{mod. } 8n + 1),$$

es posible. Representando la misma x una de sus raices, como

$$(x^4 + 1) = (x^2 \pm 1)^2 \mp 2x^2,$$

será:

$$(x^2 \pm 1)^2 \equiv \pm 2x^2 \,(\text{mod. } 8n + 1):$$

de cuya congruencia se concluye que $\pm 2x^2$, y, de consiguiente, ± 2 es resto de $8n + 1$, ó, bajo distinta forma, que:

$$\left(\frac{\pm 2}{p}\right) = +1 \quad \textit{cuando} \quad p = 8n + 1.$$

La proposicion enunciada queda resuelta en todas sus partes; pero todavía nos resta averiguar si los caractéres del número 2, sucesivamente determinados para las formas particulares de p, pudieran compendiarse en una sola ecuacion, semejante á la que para el símbolo $\left(\frac{-1}{p}\right)$ obtuvimos en el párrafo precedente. Para esto basta observar, que los cuadrados de las formas $8n \pm 1$, y $8n \pm 3$, de las cuales es 2 resto ó no-resto respectivamente, son congruentes con 1 (mod. 8), ó bien que la diferencia $p^2 - 1$, es en todos los casos divisible por 8; mas con la distincion de ser el cociente $(p^2 - 1) : 8$ un número par en el primero, esto es, cuando $p = 8n \pm 1$, y un número impar en el segundo, cuando $p = 8n \pm 3$; resultando de estos hechos que la potencia

$$(-1)^{\frac{p^2-1}{8}}$$

será la unidad positiva ó negativa, segun que p esté contenido en las unas ó las otras formas, y, por consecuencia, que la ecuacion

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

expresa el carácter general del número 2 para todas las formas que, respecto del número 8, pueden afectar los números primos impares.

114.—*Otra demostracion de este carácter.*

El método inductivo que empleamos en la demostracion anterior vimos que no era aplicable á todas las formas comprendidas en el enunciado del criterio ó carácter del número 2. Conviene, por lo tanto, que determinemos este mismo carácter por otro procedimiento igualmente riguroso, pero que abrace todos los casos á que la determinacion que buscamos pueda referirse. Este procedimiento se funda en los principios explicados (105), segun los cuales, para indagar si el número 2 es resto ó no-resto del número p, basta determinar cuántos restos mínimos positivos, mayores que $\frac{1}{2}p$, existen entre los restos (mod. p) de los $\frac{1}{2}(p-1)$ productos sucesivos de 2,

$$1.1,\ 2.2,\ 3.2,\ \ldots\ldots\ \tfrac{1}{2}(p-1).2 \quad \text{ó} \quad 2,\ 4,\ 6,\ \ldots\ldots\ (p-1).$$

Mas estos productos son ellos mismos sus restos mínimos positivos y pares (mod. p); y, por consecuencia, solamente tendremos que averiguar cuántos de ellos son mayores que $\frac{1}{2}p$.

Para esto sabemos (104) que de los $p-1$ restos de un módulo impar p, la mitad, esto es, $\frac{1}{2}(p-1)$, son pares, y la otra mitad impares. Si el número $\frac{1}{2}(p-1)$ es tambien par, entre los restos pares habrá

tantos, á saber: $\frac{1}{4}(p-1)$, superiores á $\frac{1}{2}p$, como inferiores; pero, si $\frac{1}{2}(p-1)$ fuese impar, $\frac{1}{2}\left\{\frac{1}{2}(p-1)+1\right\}=\frac{1}{4}(p+1)$ serian mayores, y $\frac{1}{2}\left\{\frac{1}{2}(p-1)-1\right\}=\frac{1}{4}(p-3)$ menores que $\frac{1}{2}p$. Luego, designando por μ el número de los restos superiores á $\frac{1}{2}p$, comprendidos en la série de los $\frac{1}{2}(p-1)$ restos pares de p, que es precisamente la de los productos de 2 arriba escrita, resulta que el valor de μ oscila, en todo caso, entre los límites $\frac{1}{4}(p-1)$ y $\frac{1}{4}(p+1)$, cuya diferencia es $\frac{2}{4}=\frac{1}{2}$, y está determinado, de consiguiente, por las condiciones

$$\frac{p-2}{4}<\mu<\frac{p+2}{4},$$

de las cuales (54) se deduce:

$$\mu=\left[\frac{p+2}{4}\right].$$

Ahora bien, segun p tenga las formas $8n+1$, $8n+3$, $8n+5$, $8n+7$, así será $\mu=2n$, $2n+1$, $2n+1$, $2n+2$, respectivamente; esto es: par, y, por consecuencia

$$\left(\frac{2}{p}\right)=+1, \quad \textit{cuando sea} \quad p\equiv\pm 1 \pmod 8;$$

impar; y, por lo tanto:

$$\left(\frac{2}{p}\right)=-1, \quad \textit{cuando sea} \quad p\equiv\pm 3 \pmod 8.$$

115.—*Determinacion del símbolo* $\left(\frac{q}{p}\right)$.—*Ley de reciprocidad.*

Mediante la trasformacion (105) del carácter de Euler acabamos de hallar para el correspondiente al número 2 una expresion de μ en funcion del módulo p. Exactamente lo mismo en el fondo vamos á buscar ahora: una expresion analítica de μ, funcion de q y p, de cuyas formas dependerá naturalmente la de aquel número.

Designando por $[x]$ el entero máximo contenido en x, definido por las condiciones

$$0 \leqq x - [x] < 1;$$

cambiando la D en q, y haciendo por abreviar $\frac{1}{2}(p-1) = p'$, ó bien $p = 2p' + 1$, los p' productos de D (105), que serán ahora de q, divididos por p, producirán las igualdades siguientes:

$$\begin{aligned}
1q &= p\left[\frac{q}{p}\right] + r_1 \\
2q &= p\left[\frac{2q}{p}\right] + r_2 \\
3q &= p\left[\frac{3q}{p}\right] + r_3 \\
&\cdots\cdots\cdots\cdots \\
&\cdots\cdots\cdots\cdots \\
p'q &= p\left[\frac{p'q}{p}\right] + r_{p'},
\end{aligned} \qquad (1)$$

en las cuales los restos

$$r_1, r_2, r_3 \ldots\ldots r_{p'},$$

se hallan comprendidos (exclusive) entre los límites 0 y p. Distribuyamos estos restos mínimos positivos de p en dos grupos, segun se hizo en el párrafo citado: el uno que comprenda los superiores á $\frac{1}{2}p$, y el otro los inferiores; representando, como allí, por

$$a_1,\ a_2,\ a_3\ \ldots\ldots\ a_\mu$$

los primeros, y por

$$b_1,\ b_2,\ b_3\ \ldots\ldots\ b_\lambda,$$

los segundos; por A la suma de los μ superiores, por B lá de los λ inferiores á $\frac{1}{2}p$, y por M la suma

$$M=\left[\frac{q}{p}\right]+\left[\frac{2q}{p}\right]+\left[\frac{3q}{p}\right]+\ldots\ldots+\left[\frac{p'q}{p}\right],$$

de los cocientes enteros que figuran en las igualdades (1); tendremos, sumando éstas:

$$(1+2+3+\ldots\ldots+p')q=\tfrac{1}{2}(p'+1)p'q=pM+A+B;$$

ó, sustituyendo por p' su valor $\frac{1}{2}(p-1)$,

$$\frac{p^2-1}{8}q=pM+A+B.$$

Por otra parte sabemos (105) que los números

$$p-a_1,\ p-a_2,\ \ldots\ldots\ p-a_\mu,\ b_1,\ b_2\ \ldots\ldots\ b_\lambda,$$

cuya suma es $\mu p-A+B$, son, prescindiendo del órden, iguales á estos otros:

$$1,\ 2,\ 3,\ \ldots\ldots\ p',\ \text{cuya suma es}\ \frac{p^2-1}{8};$$

y, por consecuencia, lo serán tambien estas sumas, esto es:

$$\frac{p^2-1}{8} = \mu p - A + B.$$

Restando esta igualdad de la anterior resulta la siguiente:

$$\frac{p^2-1}{8}(q-1) = (M-\mu)p + 2A,$$

que nos facilita los medios de conocer cuándo es μ par ó impar; pues, suprimiendo en ella los múltiplos de 2, y teniendo en cuenta que $p \equiv -1 \pmod 2$, se transforma en la congruencia

$$\mu \equiv M + \frac{p^2-1}{8}(q-1) \pmod 2;$$

y ésta ya manifiesta que μ será par ó impar, segun sea una de las dos cosas su segundo miembro.

De la misma se desprende, cuando $q = 2$, por ejemplo, en cuyo caso $M = 0$, la siguiente:

$$\mu \equiv \frac{p^2-1}{8} \pmod 2;$$

y de aquí el criterio ya conocido (113)

$$\left(\frac{2}{p}\right) = (-1)^{\mu} = (-1)^{\frac{p^2-1}{8}}.$$

Y, si admitimos en general que q sea un número impar, y entónces $q-1$ es par, esta otra:

$$\mu \equiv M \pmod 2,$$

y, por lo tanto

$$\left(\frac{q}{p}\right) = (-1)^{M};$$

es decir, que la cuestion de averiguar cuándo será μ par ó impar, se reduce, por último, á saber cuándo será lo uno ó lo otro, la suma representada por la letra M.

Para esto supongamos que, además de impar, sea q positivo é inferior á p. Entónces, como la diferencia entre dos cocientes sucesivos

$$\frac{sq}{p} \quad \text{y} \quad \frac{(s+1)q}{p},$$

es < 1, y, por consecuencia, entre ambos sólo un entero á lo sumo podrá estar comprendido, cada término de la suma M excederá en una unidad todo lo más al inmediatamente anterior. El último de estos cocientes, por otra parte, es

$$\frac{p'q}{p} = \frac{(p-1)q}{2p} = \frac{q-1}{2} + \frac{p-q}{2p};$$

y el último término de la série M, de consiguiente:

$$\left[\frac{p'q}{p}\right] = \frac{q-1}{2} = q',$$

luego los términos de dicha série ó suma M irán sucesivamente presentando los valores $0, 1, 2, \ldots\ldots q'$.

La cuestion ahora es averiguar cuántos de tales términos tendrán el valor 0, cuántos el valor 1, cuántos el valor 2..... etc.; y, para esto, hallaremos el valor de s mediante la condicion de que dos términos sucesivos,

$$\left[\frac{sq}{p}\right] \quad \text{y} \quad \left[\frac{(s+1)q}{p}\right],$$

difieren realmente en una unidad; de modo que, si el primero se supone igual á $t-1$, valga el segundo t, siendo t cualquiera de los números 1, 2, 3, ... q'. De la condicion expresada, en atencion á que ninguno de los cocientes completos $sq:p$ puede ser entero, como q es primo con p, y $s<p$, se desprenden las siguientes:

$$\frac{sq}{p}<t<\frac{(s+1)q}{p},$$

de donde se deducen:

$$s<\frac{tp}{q}<s+1, \quad \text{y, de consiguiente:} \quad s=\left[\frac{tp}{q}\right].$$

Este valor de s representa el número de términos de la série M inferiores á t; del mismo modo $\left[\frac{(t-1)p}{q}\right]$ representa el de los inferiores á $t-1$; y, por consiguiente, la diferencia

$$\left[\frac{tp}{q}\right]-\left[\frac{(t-1)p}{q}\right]$$

expresará cuántos términos de la série mencionada son iguales á $t-1$. Además, como el número total de estos términos es $p'=\frac{1}{2}(p-1)$, y el de los inferiores á $q'=\frac{1}{2}(q-1)$, segun la expresion de s, es $\left[\frac{q'p}{q}\right]$, resulta que habrá entre aquellos evidentemente $p'-\left[\frac{q'p}{q}\right]$ iguales á q'. Por lo tanto, los productos

$$(t-1)\times\left(\left[\frac{tp}{q}\right]-\left[\frac{(t-1)p}{q}\right]\right) \quad \text{y} \quad q'\left(p'-\left[\frac{q'p}{q}\right]\right)$$

representan el valor de todos los términos de la série M, iguales respectivamente á $t-1$ y á q': luego si t recibe uno á uno los valo-

res 1, 2, 3, ... $q'-1$, sumamos los productos correspondientes, y agregamos despues á ellos el segundo de los dos arriba escritos, el valor de M será:

$$= 0.\left[\frac{p}{q}\right] + 1.\left(\left[\frac{2p}{q}\right] - \left[\frac{p}{q}\right]\right) + 2.\left(\left[\frac{3p}{q}\right] - \left[\frac{2p}{q}\right]\right) + ...$$

$$..... + (q'-1).\left(\left[\frac{q'p}{q}\right] - \left[\frac{q'-1}{q}\right]\right) + q'.\left(p' - \left[\frac{q'p}{q}\right]\right);$$

ó bien, efectuando las multiplicaciones indicadas y las reducciones consiguientes:

$$M = -\left[\frac{p}{q}\right] - \left[\frac{2p}{q}\right] - \left[\frac{3p}{q}\right] - ..... - \left[\frac{q'p}{q}\right] + q'p',$$

Haciendo $N = \left[\frac{p}{q}\right] + \left[\frac{2p}{q}\right] + \left[\frac{3p}{q}\right] + ... + \left[\frac{q'p}{q}\right]$ y sustituyendo por q' y p' sus valores hallamos por fin:

$$M + N = q'p' = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

resultado que tiene lugar siempre que los números p, q, sean positivos, impares y primos entre sí: únicas condiciones que hemos exigido para obtenerlo; y, como tambien es simétrico completamente respecto de dichos números, no hay dificultad tampoco en suponer inferior al otro cualquiera de ellos. Así, pues, aunque en realidad no hayamos encontrado el valor de M que buscábamos, sino que solamente lo hemos referido al de N, basta esto, sin embargo, para establecer la ley de reciprocidad. En efecto, probamos antes que la ecuacion

$$\left(\frac{q}{p}\right) = (-1)^M$$

se verificaba siempre que fuese p un número positivo, primo é impar, y q otro número impar cualquiera, pero no divisible por p. Si suponemos ahora que q posea las mismas propiedades que atribuimos á p, tambien será cierta, segun lo dicho arriba, esta otra:

$$\left(\frac{p}{q}\right) = (-1)^{N},$$

y de ambas se deduce la siguiente:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M+N} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

que representa la LEY DE RECIPROCIDAD. Esta expresion manifiesta que los dos símbolos $\left(\frac{p}{q}\right)$ y $\left(\frac{q}{p}\right)$ tendrán igual valor, si uno, por lo ménos, de los números p y q, es de la forma $4n+1$ (en cuyo caso el exponente de (-1) es par, y la potencia $=+1$); y valores opuestos, cuando los dos números p y q sean de la forma $4n+3$ (pues entónces el exponente de (-1) es impar).

Esta ley, en lenguaje vulgar, dice así:

Si p y q representan dos números positivos, primos é impares, y uno de ellos, por lo ménos, es de la forma $4n+1$, q será resto ó no-resto de p, segun que p sea resto ó no-resto de q; pero, si los dos tienen la forma $4n+3$, q será resto ó no-resto de p, segun que p sea no-resto ó resto de q.

Atendiendo á su naturaleza dió *Legendre* á esta ley el nombre que lleva; *Gauss*, que publicó de la misma seis demostraciones (*), la llamó *Teorema fundamental*, porque comprende ella sola, segun dice él mismo, casi toda la teoría de los restos cuadráticos; *Lejeune-Dirichlet* (**) simplificó y mejoró algunas de ellas; así como tambien *Cauchy*, *Jacobi*, *Eisenstein*, *Lebesgue*, *Kronecker* y otros ilustres matemáticos han consagrado sus estudios á este teorema importantísimo; pero por muy apreciables que sean estos trabajos, es preciso que corran la suerte de otros muchos, dado el carácter de nuestro libro.

(*) Gauss, D. A. §§. 125, 145.—Id., §. 262.—Werke, B. II, pág. 1 á 55.

(**) Zahlen-Theorie, 42-51.

116.—*Casos particulares.*

1.° Si en la fórmula de esta ley hacemos $q = -1$, resulta la que ya conocíamos:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

2.° La suposicion $q = 2$ no puede hacerse en la fórmula mencionada, deducida en la de ser q impar; pero ya vimos que en este caso es $M = 0$, y

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

3.° Sean ahora $q = 3$, de la forma $4n + 3$, y $p = 3n \pm 1$: la fórmula fundamental da para este caso:

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}:$$

ó, sustituyendo por p su resto (mod. 3)

$$\left(\frac{3}{p}\right)\left(\frac{\pm 1}{3}\right) = (-1)^{\frac{p-1}{2}}.$$

Pero $+1$ es resto, y -1 no-resto de 3; luego 3 será tambien resto de todos los números primos $p = 3n + 1$, que tengan al mismo tiempo la forma $4n + 1$ (á que se refiere la ley), comprendidos en la que abraza las dos, $12n + 1$; y no-restos de los que tengan al mismo tiempo la forma $4n - 1 = 4n + 3$, comprendidos en la compuesta $12n - 5 =$

$= 12n+7$, que representa efectivamente la de los números que dan el resto 1 segun el módulo 3, y el resto $3 = -1$ segun el módulo 4. En resúmen: combinando las formas dadas, $3n \pm 1$, de p, con las dos, $4n+1$ y $4n+3$, que figuran en la ley de reciprocidad, se deduce la proposicion siguiente:

El número 3 *es resto de todos los números primos de las formas* $12n+1$ y $12n+11$; *y no-resto de todos los números primos de las formas* $12n+5$ *y* $12n+7$.

Y, segun lo demostrado (112).

El número -3 *es resto de todos los números primos de las formas* $12n+1$ y $12n+11$, *y no-resto de todos los números primos tambien de las formas* $12n+5$ y $12n+7$.

4.° Si tomamos ahora el número 5, de la forma $4n+1$, segun el teorema fundamental, será:

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right),$$

pero sabemos (106) que

$$\left(\frac{p}{5}\right) = \pm 1,$$

segun p tenga las formas $5n \pm 1$ ó $5n \pm 2$: luego, combinando estas formas con las $4n \pm 1$, resulta que:

El número 5 *es resto de todos los números primos de las formas*

$$20n+1, \quad 20n+9, \quad 20n+11, \quad 20n+19,$$

y no-resto de los comprendidos en las formas

$$20n+3, \quad 20n+7, \quad 20n+13, \quad 20n+17.$$

5.° La ley de reciprocidad, haciendo $q = 7$, de la forma $4n+3$, se particulariza y expresa de este modo:

$$\left(\frac{7}{p}\right) = \pm\left(\frac{p}{7}\right),$$

en cuya ecuacion se tomará el signo $+$ ó el $-$, segun que sea p de la forma $4n+1$, ó de la forma $4n+3$. Reasumiendo las anteriores indicaciones, estudiemos este caso, para concluir de ejemplos, bajo su aspecto más general y provechoso en lo sucesivo.

Las diferentes formas que, respecto del módulo 7, puede afectar un número primo cualquiera, son las siguientes:

$$7n+1, \quad 7n+2, \quad 7n+3, \quad 7n+4, \quad 7n+5, \quad 7n+6,$$

comprendidas en la general

$$7n+r.$$

El distinguir ahora, entre los números p que esta forma contiene, cuáles son de la $4n+1$ y cuáles de la $4n+3$, equivale á determinar dos formas numéricas que divididas por 7 den el resto r, y divididas por 4 los restos 1 ó 3; problema ya en otro lugar (72) resuelto. Las congruencias auxiliares para este caso son:

$$4\alpha \equiv 1 \pmod{7}, \quad 7\beta \equiv 1 \pmod{4};$$

de las cuales se deducen:

$$\alpha = 2, \quad \beta = 3 \equiv -1; \quad 4\alpha = 8, \quad 7\beta = 21 \equiv -7;$$

y, por consecuencia:

$$\left.\begin{array}{ll} p \equiv 8r+21 & \equiv 8r-7 \\ p \equiv 8r-21 & \equiv 8r+7 \end{array}\right\} \pmod{28}.$$

ó

Sustituyendo por r sus valores numéricos (restos mínimos absolutos), en este órden:

$$+1, \quad +2, \quad -3, \quad +3, \quad -2, \quad -1,$$

se obtienen para p los siguientes:

$$p = \begin{cases} 8r-7 \equiv & 1, & 9, & -3, & -11, & 5, & 13 \\ 8r+7 \equiv & -13, & -5, & 11, & 3, & -9, & -1 \end{cases} \pmod{28},$$

De estas formas, las seis

$$28n+1,\quad 28n+9,\quad 28n-3,\quad 28n-13,\quad 28n-5,\quad 28n+11,$$

cuyos restos (mod. 7), elevados á la potencia $\frac{1}{2}(7-1)=3$ son congruentes (mod. 7) con la unidad positiva, representan (106) los restos cuadráticos de 7; y las otras seis

$$28n-11,\quad 28n+5,\quad 28n+13,\quad 28n+3,\quad 28n-9,\quad 28n-1,$$

son no-restos de 7. Las tres primeras de los restos de 7 son tambien restos de p, por ser de la forma $4n+1$; las tres últimas son de la forma $4n+3=4n-1$, y, por consecuencia, respecto de p lo contrario que respecto de 7. Y lo mismo acontece con las del segundo grupo ó no-restos de 7: las tres primeras, de la forma $4n+1$, son tambien no-restos de p; y las tres últimas, de la forma $4n+3$, son restos de p.

En conclusion:

El número 7 *es resto de todos los números primos de las formas*

$$28n+1,\quad 28n+9,\quad 28n-3,\quad 28n+3,\quad 28n-9,\quad 28n-1;$$

y no-resto de los representados por las formas

$$28n-13,\quad 28n-5,\quad 28n+11,\quad 28n-11,\quad 28n+5,\quad 28n+13.$$

117.—*Determinacion del símbolo de Legendre mediante la ley de reciprocidad.*

El teorema fundamental, cuyas aplicaciones estamos estudiando, sirve tambien para discernir cuándo será ó no posible la congruencia de módulo primo

$$x^2 \equiv D \pmod{p}.$$

En efecto, esta congruencia será posible cuando

$$\left(\frac{D}{p}\right) = +1;$$

así que nuestro problema se reduce á determinar el signo del símbolo de Legendre $\left(\frac{D}{p}\right)$. Para esto sabemos (104) que, si el número D, despues de haber quitado de él los múltiplos de p, afecta la forma

$$D = a^{\alpha} . \; b^{\beta} . \; c^{\gamma} \; \ldots\ldots$$

será

$$\left(\frac{D}{p}\right) = \left(\frac{a^{\alpha}}{p}\right)\left(\frac{b^{\beta}}{p}\right)\left(\frac{c^{\gamma}}{p}\right)\ldots\ldots;$$

mas evidentemente

$$\left(\frac{a^{\alpha}}{p}\right) = +1 \quad \text{ó} \quad \left(\frac{a^{\alpha}}{p}\right) = \left(\frac{a}{p}\right),$$

segun α sea par ó impar: luego la determinacion del símbolo que buscamos se refiere á la de los símbolos sencillos

$$\left(\frac{a}{p}\right), \left(\frac{b}{p}\right)\ldots\ldots,$$

correspondientes á los factores primos a, b, ... que figuran en el número D (fuera los múltiplos de p), con exponentes impares.

Consideremos uno cualquiera de ellos, $\left(\frac{a}{p}\right)$, por ejemplo. Su valor en los casos particulares de ser $a = 2, 3, 5, 7$ le conocemos inmediatamente; pero, si así no fuese, por el teorema fundamental convertiríamos su determinacion en la del símbolo $\left(\frac{p}{a}\right)$. Procediendo con este

nuevo símbolo lo mismo exactamente que con el primero $\left(\frac{D}{p}\right)$, y así continuando, llegaremos precisamente á símbolos cuyo valor conozcamos.

Sea, por ejemplo, la congruencia

$$x^2 \equiv 365 \pmod{1847},$$

y, por consecuencia, el símbolo

$$\left(\frac{365}{1847}\right)$$

cuyo valor se busca. Como $365 = 5.73$, tendremos:

$$\left(\frac{365}{1847}\right) = \left(\frac{5}{1847}\right)\left(\frac{73}{1847}\right).$$

Consideremos primeramente el símbolo ó factor primero. Siendo 5 de la forma $4n+1$, segun la ley de reciprocidad será:

$$\left(\frac{5}{1847}\right) = \left(\frac{1847}{5}\right),$$

y, puesto que $1847 \equiv 2 \pmod{5}$;

$$\left(\frac{5}{1847}\right) = \left(\frac{1847}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

Para determinar el otro factor observamos que 73 es tambien de la forma $4n+1$; y teniendo en cuenta que $1847 \equiv 22 \pmod{73}$, será:

$$\left(\frac{73}{1847}\right) = \left(\frac{1847}{73}\right) = \left(\frac{22}{73}\right) = \left(\frac{2}{73}\right)\left(\frac{11}{73}\right),$$

ó bien

$$\left(\frac{73}{1847}\right) = \left(\frac{11}{73}\right);$$

en atencion á que $73 \equiv 1 \pmod{8}$, y por tanto,

$$\left(\frac{2}{73}\right) = 1.$$

Aplicando de nuevo el teorema fundamental al símbolo que falta, hallamos:

$$\left(\frac{11}{73}\right) = \left(\frac{73}{11}\right) = \left(\frac{7}{11}\right);$$

y, como 7 y 11 son de la forma $4n + 3$,

$$\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right) = -\left(\frac{2^2}{7}\right) = -1.$$

Luego, por último:

$$\left(\frac{365}{1847}\right) = \left(\frac{5}{1847}\right)\left(\frac{73}{1847}\right) = -1 \,.\, -1 = +1.$$

Este resultado prueba que la congruencia propuesta es posible; y, efectivamente:

$$(\pm 496)^2 = 246016 = 365 + 133 \,.\, 1847.$$

118.—*Generalizacion por Jacobi del símbolo de Legendre.*

Supongamos que P sea un número *impar*, descompuesto en sus factores primos p, p', p'' .....,

$$P = p.\ p'.\ p''\ .....,$$

y m otro número cualquiera, *primo con* el primero: la definicion del símbolo de *Jacobi* es la siguiente:

$$\left(\frac{m}{P}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right).....$$

Es claro que el valor de este símbolo será $+1$, ó -1, segun que sea par, ó impar, el número de los factores p, p', p'' ..... de los cuales sea m no-resto cuadrático. Si m fuese resto de P, y, por consecuencia, de cada uno de sus factores primos p, p', p'' ....., de modo que

$$\left(\frac{m}{p}\right) = \left(\frac{m}{p'}\right) = \left(\frac{m}{p''}\right)..... = +1,$$

será tambien:

$$\left(\frac{m}{P}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right)..... = +1.$$

Pero nótese que la inversa de esta ley no siempre será cierta; porque mientras m sea no-resto de dos, cuatro, seis, y, en general, de un número par de los factores p, p', p'' ..... del número P, será $+1$ el valor del símbolo $\left(\frac{m}{P}\right)$, y, sin embargo, m no-resto de P. En el supuesto de ser P un número primo, los símbolos de Jacobi y de

Legendre coinciden; y en el de ser $P = 1$, admitimos desde luego que el valor del símbolo $\left(\frac{m}{1}\right)$ es siempre la unidad positiva; con lo cual abraza nuestra definicion todos los casos posibles.

Hé aquí ahora las propiedades mas interesantes del símbolo de Jacobi que de la misma definicion se derivan.

1.ª *Si m es primo con los dos números impares P y Q, y, de consiguiente, con su producto tambien impar PQ, será*

$$\left(\frac{m}{P}\right)\left(\frac{m}{Q}\right) = \left(\frac{m}{PQ}\right).$$

Pues haciendo

$$P = p\,p'\,p''\,.\,.\,.$$

$$Q = q\,q'\,q''\,.\,.\,.\,.$$

tendremos:

$$\left(\frac{m}{PQ}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right).\,.\,.\,.\left(\frac{m}{q}\right)\left(\frac{m}{q'}\right)\left(\frac{m}{q''}\right).\,.\,.\,. = \left(\frac{m}{P}\right)\left(\frac{m}{Q}\right).$$

2.ª *Si los números l, m, n, ... son primos con P, será*

$$\left(\frac{l}{P}\right)\left(\frac{m}{P}\right)\left(\frac{n}{P}\right).\,.\,.\,.\,. = \left(\frac{l\,m\,n\,.\,.\,.\,.\,.}{P}\right).$$

Porque, haciendo segun costumbre,

$$P = p\,p'\,p''\,.\,.\,.\,.\,.$$

tendremos:

$$\left(\frac{l}{P}\right) = \left(\frac{l}{p}\right)\left(\frac{l}{p'}\right)\left(\frac{l}{p''}\right).\,.\,.\,.\,;$$

$$\left(\frac{m}{P}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right)\ldots\ldots;$$

$$\left(\frac{n}{P}\right) = \left(\frac{n}{p}\right)\left(\frac{n}{p'}\right)\left(\frac{n}{p''}\right)\ldots\ldots;$$

y, como (104)

$$\left(\frac{l}{p}\right)\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)\ldots\ldots = \left(\frac{l\,m\,n\ldots\ldots}{p}\right),$$

y lo mismo puede decirse de los demás factores p', $p''\ldots\ldots$, de P, multiplicando ordenadamente las igualdades anteriores se obtiene esta otra:

$$\left(\frac{l}{P}\right)\left(\frac{m}{P}\right)\left(\frac{n}{P}\right)\ldots\ldots = \left(\frac{l\,m\,n\ldots\ldots}{p}\right)\left(\frac{l\,m\,n\ldots\ldots}{p'}\right)\left(\frac{l\,m\,n\ldots\ldots}{p''}\right)\ldots\ldots$$

que demuestra el teorema.

3.° *Si m es primo con P (siempre impar), y $m \equiv m'$ (mod. P), y de consiguiente, m' tambien primo con P, será*

$$\left(\frac{m}{P}\right) = \left(\frac{m'}{P}\right).$$

En efecto, de la igualdad siempre admitida

$$P = p\,p'\,p''\ldots\ldots,$$

se deducen las congruencias

$$m \equiv m' \text{ (mod. } p), \quad m \equiv m' \text{ (mod. } p') \quad m \equiv m \text{ (mod. } p'')\ldots\ldots$$

y de éstas las igualdades:

$$\left(\frac{m}{p}\right) = \left(\frac{m'}{p}\right), \left(\frac{m}{p'}\right) = \left(\frac{m'}{p'}\right), \left(\frac{m}{p''}\right) = \left(\frac{m'}{p''}\right)\ldots\ldots$$

que multiplicadas ordenadamente producen la que sigue:

$$\left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right)\ldots\ldots = \left(\frac{m'}{p}\right)\left(\frac{m'}{p'}\right)\left(\frac{n'}{p''}\right)\ldots\ldots$$

que demuestra la proposicion enunciada.

119.—*Relacion entre los símbolos de Legendre y de Jacobi.*

Aunque las dos últimas proposiciones manifiestan que el símbolo generalizado obedece á las mismas leyes que el de Legendre, es importante además, y en corroboracion de esto mismo, poner á la vista la perfecta analogía que existe entre los valores de los símbolos particulares y la ley de reciprocidad, para números primos, anteriormente determinados, y los de aquellos valores y ésta ley, cuando á números compuestos se refieran. Mas antes de entrar en materia y á fin de no interrumpir despues el discurso en las demostraciones, comenzaremos por exponer los fundamentos en que hasta cierto punto se apoya.

Lema. Sea

$$R = r'\,r''\,r'''\ldots\ldots$$

un número impar cualquiera. Todos sus factores r', r'', r''' ....., serán necesariamente impares; las diferencias $r'-1$, $r''-1$, $r'''-1$ ....., por consecuencia, serán pares; y el producto de dos, ó varias de ellas, divisible por 4, ó $\equiv 0 \pmod 4$. Por lo tanto, si escribimos el producto R en la forma

$$R = [1+(r'-1)]\,.\,[1+(r''-1)].\,[1+(r'''-1)]\ldots\ldots,$$

efectuamos la multiplicacion indicada, y suprimimos los múltiplos de 4, resultará la congruencia

$$R \equiv 1+(r'-1)+(r''-1)+(r'''-1)\ldots\ldots \pmod 4.$$

ó bien (61—5.ª) esta otra más sencilla:

$$\frac{R-1}{2} = \Sigma \frac{r-1}{2} \text{ (mod. 2)}, \qquad (1)$$

en la cual se refiere el signo sumatorio á todos los factores impares r', r'', r''' ....., del producto R.

Elevando al cuadrado el producto R de los números impares r', r'', r''' .....,

$$R^2 = r'^2 r''^2 r'''^2 .....,$$

tanto dicho producto como cada uno de sus factores (todos impares), serán $\equiv 1$ (mod. 8); divisibles por 8, de consiguiente, las diferencias $R^2 - 1$ y $r'^2 - 1$, $r''^2 - 1$, $r'''^2 - 1$ .....; y los productos de dos ó varias de estas diferencias divisibles por $8 \times 8 = 64$. Luego, si damos á los factores r^2 la forma $1 + (r^2 - 1)$, obtendremos por el procedimiento que antes, la congruencia

$$R^2 \equiv 1 + \Sigma (r^2 - 1) \text{ (mod. 64)}. \ (*)$$

y tambien esta otra:

$$\frac{R^2 - 1}{8} \equiv \Sigma \frac{r^2 - 1}{8} \text{ (mod. 8)},$$

y con mayor razon la siguiente;

$$\frac{R^2 - 1}{8} \equiv \Sigma \frac{r^2 - 1}{8} \text{ (mod. 2)}. \qquad (2)$$

(*) Si designamos por Πr el producto R de los números impares r', r'', r''' ....., será tambien

$$\Pi r - \Sigma (r-1) \equiv 1 \text{ (mod. 4)} \quad \text{y} \quad \Pi r^2 - \Sigma (r^2 - 1) \equiv \text{(mod. 64)}.$$

Hechas estas consideraciones, determinemos ya el valor de los símbolos á que al principio del párrafo aludimos.

1.° Representando P un número impar positivo, será

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{p-1}{2}}.$$

En efecto, descomponiendo P en sus factores primos p', p'', p'''..... segun la definicion del símbolo de Jacobi, tendremos:

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{p'}\right)\left(\frac{-1}{p''}\right)\left(\frac{-1}{p'''}\right)..... = (-1)^{\Sigma\frac{p-1}{2}}$$

refiriéndose el signo sumatorio á todos los factores de P; y, como estos factores son impares, es aplicable la congruencia (1), que se convierte para este caso en la siguiente:

$$\Sigma\frac{p-1}{2} \equiv \frac{P-1}{2} \pmod{2};$$

luego

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}.$$

2.° Si P es un número impar, será tambien

$$\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}},$$

pues en este caso tendremos:

$$\left(\frac{2}{P}\right) = \left(\frac{2}{p'}\right)\left(\frac{2}{p''}\right)\left(\frac{2}{p'''}\right)\ldots\ldots = (-1)^{\Sigma\frac{P^2-1}{8}};$$

y, segun la congruencia (2),

$$\Sigma\,\frac{p^2-1}{8} \equiv \frac{P^2-1}{8} \pmod 2:$$

luego

$$\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}.$$

3.° Si P y Q representan dos números impares, positivos y primos entre sí, tendremos tambien la ley:

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

En efecto, siendo

$$P = p'\,p''\,p'''\ldots\ldots$$

$$Q = q'\,q''\,q'''\ldots\ldots$$

y los factores primos $q', q''\ldots\ldots$ de Q, diferentes de los $p', p''\ldots\ldots$ de P, segun la definicion del símbolo de Jacobi y la propiedad del mismo (2.ª), tendremos:

$$\left(\frac{P}{Q}\right) = \left(\frac{P}{q'}\right)\left(\frac{P}{q''}\right)\ldots\ldots = \left(\frac{p'}{q'}\right)\left(\frac{p''}{q'}\right)\ldots\ldots\left(\frac{p'}{q''}\right)\left(\frac{p''}{q''}\right)\ldots\ldots = \Pi\left(\frac{p}{q}\right);$$

refiriéndose el signo-producto Π á todas las combinaciones posibles de cada uno de los factores p de P con cada uno de los factores q de Q. Y del mismo modo:

$$\left(\frac{Q}{P}\right) = \left(\frac{Q}{p'}\right)\left(\frac{Q}{p''}\right)\ldots\ldots = \left(\frac{q'}{p'}\right)\left(\frac{q''}{p'}\right)\ldots\ldots\left(\frac{q'}{p''}\right)\left(\frac{q''}{p''}\right)\ldots\ldots = \Pi\left(\frac{q}{p}\right),$$

y de consiguiente:

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \Pi\left(\frac{p}{q}\right).\Pi\left(\frac{q}{p}\right) = \Pi\left(\frac{p}{q}\right)\left(\frac{q}{p}\right).$$

Ahora bien, conforme á la ley de reciprocidad, es:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

y, por tanto:

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\Sigma\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

comprendiendo el signo sumatorio, como antes, todas las combinaciones de cada uno de los factores p con cada uno de los factores q. Pero de este significado del signo Σ se desprende evidentemente la igualdad

$$\Sigma\frac{p-1}{2}\cdot\frac{q-1}{2} = \Sigma\frac{p-1}{2} \times \Sigma\frac{q-1}{2},$$

y, como segun la congruencia (1) del lema precedente, es:

$$\begin{aligned}\Sigma\frac{p-1}{2} &\equiv \frac{P-1}{2} \\ &\qquad\qquad \text{(mod. 2)}, \\ \Sigma\frac{q-1}{2} &\equiv \frac{Q-1}{2}\end{aligned}$$

y, por consecuencia:

$$\Sigma \frac{p-1}{2} \cdot \frac{q-1}{2} \equiv \frac{P-1}{2} \cdot \frac{Q-1}{2} \text{ (mod. 2)},$$

resulta finalmente:

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}};$$

fórmula que representa una ley de reciprocidad más ámplia, semejante en todo á la de Legendre.

Réstanos advertir que la definicion del símbolo de Jacobi puede extenderse tambien al caso de ser P negativo, con tal que permanezca la condicion de ser m primo con P. En tal supuesto, el símbolo

$$\left(\frac{m}{-P}\right) \text{ es igual al símbolo } \left(\frac{m}{P}\right)$$

respecto de todas las propiedades demostradas (118); pero en cuanto á los caracteres de los números -1 y 2 referidos al producto P, y á la ley de reciprocidad generalizada, nótase bien pronto que el valor del primero exige que P sea positivo; que el del segundo es cierto, sea Q positivo ó negativo; y, por último, que la ley de reciprocidad permanecerá exacta mientras uno de los dos números P y Q, por lo ménos, se considere positivo, y perderá su exactitud cuando ambos se supongan negativos.

120.—*Determinacion del símbolo de Jacobi mediante la ley de reciprocidad generalizada.*

El problema resuelto (117) es evidentemente un caso particular del enunciado en este epígrafe; pero con la diferencia que la descomposicion en factores primos del número D, despues de reducido á su resto

mínimo (mod. p), exigida en el primero, es inútil (con excepcion del factor 2) en el segundo, en cuya resolucion vamos á emplear un algoritmo enteramente análogo al que se usa para hallar el máximo comun divisor de dos números. La sencillez de este método se hará patente por unos cuantos ejemplos.

1.° Tomemos primeramente el mismo que en el párrafo ya citado resolvimos. Segun la ley de reciprocidad generalizada será:

$$\left(\frac{365}{1847}\right) = \left(\frac{1847}{365}\right);$$

puesto que 365 es de la fórmula $4n+1$. Por otra parte

$$\left(\frac{1847}{365}\right) = \left(\frac{22}{365}\right) = \left(\frac{2}{365}\right)\left(\frac{11}{365}\right);$$

por ser $1847 \equiv 22 \pmod{365}$, y en virtud de las propiedades 3.ª y 2.ª (118); y, como $365 \equiv 5 \pmod 8$, será (2.°):

$$\left(\frac{2}{365}\right) = -1.$$

Aplicando de nuevo la ley de reciprocidad generalizada tendremos:

$$\left(\frac{11}{365}\right) = \left(\frac{365}{11}\right) = \left(\frac{2}{11}\right) = -1,$$

por ser $365 \equiv 2 \pmod{11}$, y 11 de la forma $8n+3$. Luego

$$\left(\frac{365}{1847}\right) = -1.-1 = +1.$$

2.° Conforme á la ley de reciprocidad generalizada, se verifica la igualdad

$$\left(\frac{195}{1901}\right) = \left(\frac{1901}{195}\right);$$

puesto que 1901 es de la forma $4n+1$. Como $1901 \equiv -49 \pmod{195}$, será

$$\left(\frac{1901}{195}\right) = \left(\frac{-49}{195}\right),$$

para cuyos dos últimos números -49 y 195, de los cuales uno solo es negativo, se verifica tambien la ley de reciprocidad generalizada, y podremos, en consecuencia, restablecer la igualdad

$$\left(\frac{-49}{195}\right) = -\left(\frac{195}{-49}\right) = -\left(\frac{195}{49}\right),$$

en virtud de que -49 y 195 son ambos de la forma $4n+3$.

Aplicando de nuevo la mencionada ley, teniendo presente que $195 \equiv -1 \pmod{49}$, y que 49 es de la forma $4n+1$, resulta:

$$\left(\frac{195}{49}\right) = \left(\frac{-1}{49}\right) = +1.$$

Y en conclusion:

$$\left(\frac{195}{1901}\right) = -1.$$

La descomposicion en factores hubiera facilitado la resolucion de

este problema; pues, siendo $49 = 7^2$, desde luego habríamos hallado.

$$\left(\frac{-49}{195}\right) = \left(\frac{-1}{195}\right) = -1,$$

sin otra operacion sino la de suprimir el cuadrado 49 (cosa siempre posible, como sabemos, sea cualquiera el término en que los factores cuadrados se hallen), del numerador del símbolo $\left(\frac{-49}{195}\right)$ igual al propuesto.

3.° Sea, por fin, el símbolo cuyo valor buscamos

$$\left(\frac{74}{101}\right).$$

Como $74 = 2.37$, y 101 es de la forma $8n+5$, hallamos desde luego:

$$\left(\frac{74}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{37}{101}\right) = -\left(\frac{37}{101}\right).$$

Segun la ley de reciprocidad tenemos ahora:

$$\left(\frac{37}{101}\right) = \left(\frac{101}{37}\right) = \left(\frac{-10}{37}\right) = \left(\frac{10}{37}\right):$$

y, por ser 37 de la forma $8n+5$:

$$\left(\frac{10}{37}\right) = \left(\frac{2}{37}\right)\left(\frac{5}{37}\right) = -\left(\frac{5}{37}\right).$$

Volviendo á aplicar la misma ley hallamos:

$$\left(\frac{5}{37}\right)=\left(\frac{37}{5}\right)=\left(\frac{2}{5}\right)=-1:$$

y por consecuencia:

$$\left(\frac{74}{101}\right)=-1.$$

El mismo resultado se encuentra más brevemente mediante la serie de operaciones que á continuacion se expresa:

$$\left(\frac{74}{101}\right)=\left(\frac{-27}{101}\right)=\left(\frac{101}{-27}\right)=\left(\frac{-7}{27}\right)=\left(\frac{27}{-7}\right)=\left(\frac{-1}{7}\right)=-1.$$

121.—*Formas lineales de los divisores de* t^2-Du^2.

El segundo problema que comprende la teoría de los restos cuadráticos (103), expresado bajo otro aspecto (111), despues de las últimas investigaciones se resuelve del modo siguiente. Su enunciado es:

Hallar los números primos impares q, *de los cuales el número conocido* D, *sea resto cuadrático* (refiriéndonos aquí tambien á los números primos positivos q, no contenidos en D).

Como estos números primos positivos, y primos con D, en el caso de ser $D=a^2D'$, son divisores de x^2-D del mismo modo que de x^2-D', supondremos para en adelante que el número D no contiene ningun cuadrado, excepto la unidad. En esta hipótesis, si designamos por P el producto de todos los factores primos impares p, p', p''..... de D, este número podrá ser representado por $\pm P$, ó por $\pm 2P$; de donde, prescindiendo del particular en que D no con-

tenga ningun factor primo impar, para el cual es $P = 1$, ya considerado (118), resulta que, segun sea P de la forma $4n+1$, ó de la $4n+3$, el número D afectará una de las cuatro siguientes:

$$D = \pm P \equiv 1 \pmod 4, \quad D = \pm P \equiv 3 \pmod 4;$$

$$D = \pm 2P \equiv 2 \pmod 8, \quad D = \pm 2P \equiv 6 \pmod 8;$$

que señalan los cuatro casos que por su órden estudiaremos.

I. $D = \pm P \equiv 1 \pmod P$.

En éste, si n representa un número cualquiera *positivo,* primo con $2D$ (é impar por consiguiente), conforme á la ley de reciprocidad generalizada, tendremos:

$$\left(\frac{D}{n}\right) = \left(\frac{n}{P}\right).$$

Ahora bien, como el signo del segundo miembro es el mismo para todos los números pertenecientes á la misma clase (118—3.ª) respecto de P, solamente habrá que determinar el valor de dicho símbolo para cada uno de los $\varphi(P)$ números m, incongruentes (mod. P), y primos con este módulo. Pero el valor de dicho símbolo expresa si n es resto ó no-resto de P; y, por consecuencia, lo primero que debemos probar es que entre los $\varphi(P)$ números m, incongruentes (mod. P), existen restos y no-restos de P, y, si existen, averiguar cuántos son unos y otros. La cosa es evidente cuando P no contenga sino un solo factor primo p, pues ya demostramos (106) que entónces entre los números incongruentes del sistema completo (mod. p) hay $\frac{1}{2}(p-1)$ *restos* cuadráticos de p, y otros tantos *no-restos.* Supongamos, pues, que P contenga un factor primo p, por lo menos, lo cual es de necesidad en virtud de que no puede ser $D = +1$, y designemos por β un *no-res-*

to, que ya sabemos existe, de aquel factor p. Si hacemos, en general, $P = p P'$ y determinamos un número b mediante las congruencias (72)

$$b \equiv \beta \pmod{p} \qquad b \equiv 1 \pmod{P'},$$

tendremos:

$$\left(\frac{b}{P}\right) = \left(\frac{b}{p}\right)\left(\frac{b}{P'}\right) = \left(\frac{\beta}{p}\right)\left(\frac{1}{P'}\right) = -1:$$

y esto manifiesta que el número b es *no-resto* de P. Sentado ya que existen números b, para los cuales se verifica la ecuacion

$$\left(\frac{b}{P}\right) = -1, \qquad (1)$$

no es difícil hallar que su conjunto es igual á $\frac{1}{2}\varphi(P)$; y, de consiguiente, que el de los números incongruentes $a \pmod{P}$, que satisfacen á esta otra condicion:

$$\left(\frac{a}{P}\right) = +1, \qquad (2)$$

es tambien el mismo. Escribamos para esto la igualdad

$$S = \Sigma\left(\frac{m}{P}\right),$$

donde m puede recorrer el sistema completo de los $\varphi(P)$ números incongruentes (mod. P), y primos con este módulo. Es claro que el valor de la suma S es independiente, en último resultado, de la eleccion ó el orden en que se tomen sucesivamente para m todos los individuos

que representen cada una de las clases en que aquel sistema puede distribuirse; y como, si b designa uno de aquellos individuos que cumplen con la condicion (1), el producto bm (siendo m susceptible de recibir los valores que hemos dicho) representa asimismo un sistema completo de números incongruentes y primos con P, será tambien

$$S = \Sigma\left(\frac{bm}{P}\right) = \left(\frac{b}{P}\right)\Sigma\left(\frac{m}{P}\right) = -S;$$

y, por lo tanto:

$$\Sigma\left(\frac{m}{P}\right) = 0. \qquad (3)$$

Luego el conjunto de los términos de esta suma que tienen el valor $+1$ es igual al de los que tienen el valor -1; esto es: el número de las clases a es igual al de las clases b, ó igual á $\frac{1}{2}\varphi(P)$.

Así, siempre que n represente un número congruente (mod. P) con uno de los que hemos designado por a y definido por la condicion (2), el símbolo $\left(\frac{D}{n}\right)$ será $= +1$; y será $= -1$, cuando n exprese un individuo de las clases b, ó congruente con uno cualquiera de los $\frac{1}{2}\varphi(P)$ representantes de estas clases. Pero nótese además que estos representantes a y b pueden tomarse siempre *impares;* pues, si uno cualquiera de ellos m fuese *par*, á su misma clase perteneceria el impar $m + P$; y con esta advertencia se concluye que:

$$\left(\frac{D}{n}\right) = +1, \quad \text{cuando} \quad n \equiv a \,(\text{mod. } 2P);$$

$$\left(\frac{D}{n}\right) = -1, \qquad\qquad n \equiv b \,(\text{mod. } 2P).$$

Es decir, que cualquiera número n, primo con $2D$, se halla contenido en una sola de las series aritméticas ó formas lineales,

$$2Dx+a \quad \text{ó} \quad 2Dx+b,$$

cuya diferencia es $2D$, y en las cuales representa x un número entero.

Ejemplo 1.° Sea $D=+P=21$: los $\varphi(P)=12$ números primos con 21, reducidos á sus restos mínimos absolutos, son:

$$\pm 1,\ \pm 2,\ \pm 4,\ \pm 5,\ \pm 8,\ \pm 10.$$

Hallando para cada uno de estos números el valor del símbolo de Jacobi, resultan:

$$a \equiv \pm 1,\ \pm 4, \pm 5; \qquad b \equiv \pm 2,\ \pm 8,\ \pm 10,$$

y, por consecuencia, tomando los impares exclusivamente:

$$\left(\frac{21}{n}\right) = +1, \quad \text{cuando} \quad n \equiv 1,\ 5,\ 17,\ 25,\ 37,\ 41 \pmod{42};$$

$$\left(\frac{21}{n}\right) = -1, \qquad\qquad n \equiv 11,\ 13,\ 19,\ 23,\ 29,\ 31 \pmod{42}.$$

Los números n, primos con $2D=42$, de los cuales es 21 resto cuadrático, se hallan contenidos en las seis series:

$$42x+1,\ 5,\ 17,\ 25,\ 37,\ 41;$$

y aquellos otros, de los cuales es 21 no-resto, en las siguientes:

$$42x+11,\ 13,\ 19,\ 23,\ 29,\ 31.$$

2.° Sea $D = -P = -15$. Los números inferiores y primos con 15, reducidos á sus restos mínimos absolutos, son:

$$\pm 1,\ \pm 2,\ \pm 4,\ \pm 7,$$

los cuales se distribuyen en las dos clases siguientes:

$$a \equiv +1,\ +2,\ +4,\ -7; \qquad b \equiv -1,\ -2,\ -4,\ +7;$$

y, por consecuencia:

$$\left(\frac{-15}{n}\right) = +1, \quad \text{cuando} \quad n \equiv 1,\ 17,\ 19,\ 23 \pmod{30};$$

$$\left(\frac{-15}{n}\right) = -1, \qquad\qquad n \equiv 7,\ 11,\ 13,\ 29 \pmod{30}.$$

II. $D = \pm P \equiv 3 \pmod 4$.

Designando, como antes, por n un número positivo, primo con $2D$, tendremos, segun la ley de reciprocidad generalizada:

$$\left(\frac{D}{n}\right) = (-1)^{\frac{n-1}{2}} \left(\frac{n}{D}\right) = (-1)^{\frac{n-1}{2}} \left(\frac{n}{P}\right),$$

y esto prueba que será:

$$\left(\frac{D}{n}\right) = +1, \quad \text{cuando} \quad n \equiv 1 \pmod 4 \quad \text{y} \quad n \equiv a \pmod P,$$

$$\text{ó} \qquad n \equiv 3 \pmod 4 \qquad n \equiv b \pmod P.$$

y, por el contrario:

$$\left(\frac{D}{n}\right) = -1, \quad \text{cuando} \quad n \equiv 1 \pmod 4 \quad \text{y} \quad n \equiv b \pmod P,$$

$$\text{ó} \qquad n \equiv 3 \pmod 4 \qquad n \equiv a \pmod P.$$

Cada par de estas congruencias determina (72) una clase de números n respecto del módulo $4P$; y dando á las letras a y b todos los valores que pueden recibir, se obtendrán $\varphi(P) = \frac{1}{2}\varphi(4P)$ clases de números n, pertenecientes á una misma categoría, y otras tantas clases de números n que corresponderán á la categoría opuesta, es decir, que poseerán carácter opuesto al de los comprendidos en la primera. Las clases de números n para los cuales sea $\left(\frac{D}{n}\right) = +1$, formarán progresiones aritméticas, cuya espresion abreviada es

$$4Px + \alpha;$$

y las clases de números n para los cuales sea $\left(\frac{D}{n}\right) = -1$, otras progresiones cuyo término general es

$$4Px + \beta,$$

representando α y β juntos todos los $\varphi(4P)$ números inferiores y primos con $4P$. Ambas á dos especies de progresiones tienen la diferencia comun $4D$ —.

Este mismo resultado es aplicable tambien al caso $D = -1$; pero con la diferencia de que entónces no existe ningun número de los que hemos designado por b.

Ejemplo. Sea $D = +15$. Segun vimos antes tendremos:

$$\left(\frac{D}{n}\right) = +1, \text{cuando } n \equiv 1 \pmod 4 \text{ y } n \equiv +1, +2, +4, -7 \pmod{15},$$

$$\text{ó} \quad n \equiv 3 \pmod 4 \text{ y } n \equiv -1, -2, -4, +7 \pmod{15};$$

$$\left(\frac{D}{n}\right) = -1, \text{cuando } n \equiv 1 \pmod 4 \text{ y } n \equiv -1, -2, -4, +7 \pmod{15},$$

$$\text{ó} \quad n \equiv 3 \pmod 4 \text{ y } n \equiv +1, +2, +4, -7 \pmod{15};$$

de lo cual se deduce:

$$\left(\frac{15}{n}\right) = +1, \quad \text{cuando} \quad n \equiv 1, 7, 11, 17, 43, 49, 53, 59 \pmod{60},$$

$$\left(\frac{15}{n}\right) = -1, \qquad n \equiv 13, 19, 23, 29, 31, 37, 41, 47 \pmod{60}.$$

Las series aritméticas correspondientes á las dos categorías de estos números n no hay necesidad de escribirlas.

III. $D = \pm 2P \equiv 2 \pmod 8$.

Representando n en este caso un número positivo, primo con D, y siendo $\pm P \equiv 1 \pmod 4$, tendremos:

$$\left(\frac{D}{n}\right) = \left(\frac{2}{n}\right)\left(\frac{\pm P}{n}\right) = (-1)^{\frac{n^2-1}{8}}\left(\frac{n}{P}\right);$$

es decir que, además de la relacion entre n y P, hemos de considerar tambien la que existe entre n y 8.

Así resulta que será:

$$\left(\frac{D}{n}\right) = +1, \quad \text{cuando} \quad n \equiv \pm 1 \pmod 8 \quad \text{y} \quad n \equiv a \pmod P,$$

$$\text{ó} \qquad n \equiv \pm 3 \pmod 8 \quad \text{y} \quad n \equiv b \pmod P;$$

y por el contrario:

$$\left(\frac{D}{n}\right) = -1, \quad \text{cuando} \quad n \equiv \pm 1 \pmod 8 \quad \text{y} \quad n \equiv b \pmod P,$$

$$\text{ó} \qquad n \equiv \pm 3 \pmod 8 \quad \text{y} \quad n \equiv a \pmod P.$$

Mediante cada par de estas congruencias se determina una sola clase de números n, respecto del módulo $8P$; y, como en los cuatro pares primeros, correspondientes á los números de la categoría ó carácter $\left(\frac{D}{n}\right) = +1$, y lo mismo en los cuatro últimos de la categoría opuesta, a y b pueden en suma recibir $\varphi(P)$ valores, se concluye que los números n, para los cuales $\left(\frac{D}{n}\right) = +1$, se hallan contenidos en $2\varphi(P) = \frac{1}{2}\varphi(8P)$ clases ó progresiones aritméticas, y en otras tantas los números n, para los cuales $\left(\frac{D}{n}\right) = -1$, cuya diferencia comun es $4D$.

Ejemplo. Sea $D = -b$, y P, de consiguiente, $= 3$. Considerando en este ejemplo los números primos con 24, se halla que

$$\left(\frac{-6}{n}\right) = +1, \quad \text{cuando} \quad n \equiv 1, \ 5, \ 7, \ 11 \pmod{24},$$

$$\left(\frac{-6}{n}\right) = -1, \qquad n \equiv 13, \ 17, \ 19, \ 23 \pmod{24}.$$

IV. $D = \pm 2P \equiv 6 \pmod 8$.

En este caso es $\pm P \equiv 3 \pmod 4$, y, por consecuencia:

$$\left(\frac{D}{n}\right) = \left(\frac{-2}{n}\right)\left(\frac{\mp P}{n}\right) = (-1)^{\frac{n^2-1}{8}+\frac{n-1}{2}}\left(\frac{n}{P}\right),$$

de donde se deduce:

$$\left(\frac{D}{n}\right) = +1, \quad \text{cuando} \quad n \equiv 1, 3 \pmod 8 \quad \text{y} \quad \equiv a \pmod P,$$
$$\text{ó} \qquad\quad n \equiv 5, 7 \pmod 8 \quad \text{y} \quad \equiv b \pmod P;$$

y, por el contrario:

$$\left(\frac{D}{n}\right) = -1, \quad \text{cuando} \quad n \equiv 1, 3 \pmod 8 \quad \text{y} \quad \equiv b \pmod P,$$
$$\text{ó} \qquad\quad n \equiv 5, 7 \pmod 8 \quad \text{y} \quad \equiv a \pmod P.$$

Los números n, pues, se dividen en dos categorías: una que comprende $\frac{1}{2}\varphi(8P)$ series aritméticas, en las cuales se hallan contenidos los caracterizados por el símbolo $\left(\frac{D}{n}\right) = +1$; y otra con otras tantas séries de los números sometidos á la condicion $\left(\frac{D}{n}\right) = -1$. Ambas categorías de séries tienen la diferencia comun $4D$.

Ejemplo. Sea $D = 6$ y, por tanto, $P = 3$, tendremos:

$$\left(\frac{6}{n}\right) = +1, \quad \text{cuando} \quad n \equiv 1, \ 3, \ 19, \ 28 \pmod{24},$$

$$\left(\frac{6}{n}\right) = -1, \qquad\qquad n \equiv 7, \ 11, \ 13, \ 17 \pmod{24}.$$

Para concluir notaremos que los cuatro casos considerados pueden compendiarse y ser expresados mediante una sola ecuacion ó fórmula general. Para esto designemos por δ y ε la unidad positiva y negativa, bajo las condiciones de ser $\delta = +1$ ó -1, segun sea $\pm P \equiv 1$ ó $\equiv 3 \pmod 4$; y $\varepsilon = +1$ ó -1, al mismo tiempo que D sea impar ó par. Los cuatro casos mencionados pueden entónces expresarse del modo siguiente:

$$D = \pm P \equiv 1 \pmod 4, \quad \delta = +1, \quad \varepsilon = +1,$$

$$D = \pm P \equiv 3 \pmod 4, \quad \delta = -1, \quad \varepsilon = +1.$$

$$D = \pm 2P \equiv 2 \pmod 8, \quad \delta = +1, \quad \varepsilon = -1.$$

$$D = \pm 2P \equiv 6 \pmod 8, \quad \delta = -1, \quad \varepsilon = -1.$$

Y, segun la ley de reciprocidad generalizada, y demás leyes referentes al simbolo de Jacobi (118), tendremos:

$$\left(\frac{D}{n}\right) = \delta^{\frac{n-1}{2}} \varepsilon^{\frac{n^2-1}{8}} \left(\frac{n}{P}\right),$$

en cuya expresion general n representa un número positivo, primo con $2D$.

Si suponemos que n reciba los valores de un sistema completo de números incongruentes, segun el módulo $4D$, que sean al mismo tiempo positivos y primos con $2D$, en los cuatro casos será la suma

$$\Sigma \left(\frac{D}{n}\right) = 0.$$

Para el primer caso esta igualdad se verifica ó queda satisfecha sustituyendo por n todos los restos de este sistema completo, segun el módulo $2D$.

CAPITULO V.

De la division del círculo.

Como aplicacion de las leyes numéricas, demostradas en los capítulos precedentes, vamos á estudiar en éste una cuestion que pone de manifiesto el íntimo enlace entre asuntos al parecer muy distintos, y la utilidad y trascendencia tambien de las, en concepto de algunos matemáticos, estériles investigaciones aritméticas.

122.—*Planteamiento del problema.*

El que tratamos de resolver se reduce á *señalar sobre la circunferencia cierto número de puntos equidistantes.*

a) Considerémoslo resuelto, y dividida ya la circunferencia en n partes iguales. Este número n podremos suponer además que es *impar;* porque, si no lo fuese, $\frac{n}{2}$, ó $\frac{n}{4}$..... lo serian forzosamente, y sobre el primero de estos submúltiplos *impares* de n versarian todos nuestros razonamientos.

Si marcamos por

$$a_1 \cdot a_2 \cdot a_3 \ldots\ldots a_n \cdot$$

los puntos de division sobre la circunferencia, y los unimos sucesivamente por rectas, formaremos con éstas el polígono regular inscrito, *n-ágono*, cuyo lado será la cuerda de uno de los n arcos ó partes iguales en que el círculo se considera dividido. Y conocida la longitud de esta cuerda, es evidente que el problema está resuelto. Pero adviértase que no es necesario conocer precisamente el lado del *n-ágono*, ó la cuerda del arco $\frac{2\pi}{n}$; pues, en rigor, basta conocer la cuerda

del arco $\frac{2k\pi}{n}$, siendo k primo con n: porque, llevando esta cuerda sobre la circunferencia desde el punto a_1, por ejemplo, hasta encontrar de nuevo este punto de partida, habremos marcado sobre la periferia los n puntos que deseamos. La figura ó polígono determinado por las posiciones sucesivas, siempre en el mismo sentido, de una de estas cuerdas, correspondientes á los arcos que comprendan un número, k, de partes de la circunferencia, primo con el total n de estas partes, se denomina *polígono estrellado.*

Cualquiera que sea el número k, la longitud de la cuerda del arco compuesto por k partes de la circunferencia, y comprendido entre los límites 0 y π, será siempre igual al duplo del *seno* de la mitad de dicho arco, esto es, igual á $2R\,sen.\,\frac{k\pi}{n}$, en general, ó igual á $2R\,sen.\frac{2\pi}{n}$, si damos á k el valor particular 2; en cuyo caso será la incógnita del problema el seno de una de las divisiones de la circunferencia; pues el rádio, R, de la misma es conocido.

El cálculo de la funcion trigonométrica indicada, y áun de otras mediante las cuales pueda determinarse la primera, es muy sencillo en algunos casos. Así, por ejemplo, sabido que el *seno* de 90°, ó de $\frac{\pi}{2}$, vale 1, fácilmente se calcularán los *senos* y *cosenos* de los arcos $\frac{\pi}{4}, \frac{\pi}{8}, \frac{\pi}{16}$..... y los de sus múltiplos. La Geometría elemental nos enseña, en efecto, que los lados del cuadrado, del triángulo y del exágono, suponiendo el rádio igual á la unidad, valen respectivamente $\sqrt{2}$, $\sqrt{3}$, y 1: luego

$$sen.\frac{\pi}{4} = cos.\frac{\pi}{4} = \tfrac{1}{2}\sqrt{2}; \qquad sen.\frac{\pi}{3} = cos.\frac{\pi}{6} = \tfrac{1}{2}\sqrt{3};$$

$$y \qquad sen.\frac{\pi}{6} = cos.\frac{\pi}{3} = \tfrac{1}{2}:$$

y de estos valores se deducen los de sus múltiplos correspondientes.

Designando por x la longitud del lado del decágono (inscrito como los anteriores), sabemos tambien que su valor se deduce de la ecuacion

$$x^2 = 1 \times (1 - x) \quad \text{ó bien de la} \quad x^2 + x - 1 = 0 ,$$

y es, por consecuencia, refiriéndonos al polígono ordinario,

$$x = \frac{-1 + \sqrt{5}}{2} .$$

Con este dato se calculan las funciones

$$\text{sen.}\frac{\pi}{10} = \cos.\frac{2\pi}{5} = \frac{-1 + \sqrt{5}}{4}; \quad \cos.\frac{\pi}{10} = \text{sen.}\frac{2\pi}{5} =$$

$$= \frac{\sqrt{10 + 2\sqrt{5}}}{4};$$

y, por éstas, las de sus arcos múltiples.

Por último, de la igualdad evidente

$$\frac{\pi}{15} = \frac{\pi}{6} - \frac{\pi}{10} .$$

se desprende que conocidas, como lo son ya, las líneas trigonométricas de los arcos $\frac{\pi}{6}$ y $\frac{\pi}{10}$, fácilmente se calcularán las del arco $\frac{\pi}{15}$ y las de sus múltiplos.

Conclúyese de lo dicho que, por los medios que nos proporciona la Geometría elemental, logramos dividir la circunferencia en cualquiera número de partes iguales espresado por una de las formas

$$2^m . \quad 3.2^m . \quad 5.2^m . \quad 15.2^m :$$

representando en ellas m todos los números enteros. 0, 1, 2.....

Dos mil años despues de haber Euclides publicado estas soluciones geométricas, generalizó *Gauss* (*) el problema y lo convirtió en algebráico, adoptando para esto como incógnita, no ya las funciones trigonométricas simples, sino la compleja

$$\cos.\frac{2\pi}{n} + i\,\text{sen.}\frac{2\pi}{n},$$

siendo $i = \sqrt{-1}$, mediante la cual, una vez conocida, se determinan aquellas.

Para hallar, pues, un valor de esta nueva incógnita compleja, recordaremos la fórmula de *Moivre*, referida á un arco cualquiera a,

$$(\cos. a + i\,\text{sen.}\, a)^n = \cos. n\,a + i\,\text{sen.}\, n\,a.$$

Aplicando esta fórmula al arco $\frac{2\pi}{n}$, se obtiene la siguiente:

$$\left(\cos.\frac{2\pi}{n} + i\,\text{sen.}\frac{2\pi}{n}\right)^n = 1:$$

la cual demuestra que la cantidad compleja cuyo valor buscamos, es una raiz de la ecuacion binomia

$$x^n - 1 = 0. \qquad (1)$$

Mas todas las raices de esta ecuacion estan compendiadas en la forma general

$$\cos.\frac{2k\pi}{n} + i\,\text{sen.}\frac{2k\pi}{n}. \qquad (k)$$

á condicion de que la letra k reciba sucesivamente los valores

(*) D. A., Sectio septima.

0, 1, 2..... $n-1$; y esto prueba, en efecto, que el problema de la division de la circunferencia en n partes iguales se reduce á la resolucion algebráica de la ecuacion (1), cuyas soluciones representan los valores de las líneas trigonométricas, mediata ó inmediatamente, del arco $\frac{2k\pi}{n}$.

b) Así como hemos admitido antes para incógnita la cantidad compleja

$$\cos.\frac{2\pi}{n}+i\,\text{sen.}\frac{2\pi}{n},$$

tambien pudiéramos admitir la funcion simple

$$\cos.\frac{2\pi}{n}.$$

y hallar la ecuacion equivalente cuyas raices determinarian sus valores. En efecto, la ecuacion (1) tiene por raiz la unidad, que es precisamente el valor que toma la forma (k) para $k=0$; suprimiendo esta raiz, ó dividiendo dicha ecuacion (1) por el binomio $(x-1)$, el cociente resultante

$$\frac{x^n-1}{x-1}=x^{n-1}+x^{n-2}+\ldots\ldots+x+1=0 \qquad (2)$$

contendrá todas las demás raices.

Esta última ecuacion pertenece á la especie de las que se llaman *reciprocas*, esto es, de aquellas que no se alteran por cambiar la x en $\frac{1}{x}$. Haciendo en ella $n=2m+1$, y por tanto, $m=\frac{1}{2}(n-1)$, dividiéndola por x^n, y estableciendo despues la igualdad $x+\frac{1}{x}=y$, se convierte en la siguiente:

$$y^m + y^{m-1} - (m-1)\,y^{m-2} - (m-2)\,y^{m-3} +$$

$$+ \frac{(m-2)\,(m-3)}{1\,.\,2}\,y^{m-4} + \frac{(m-3)\,(m-4)}{1\,.\,2}\,y^{m-5} - \ldots\ldots = 0\,. \qquad (3)$$

Ahora bien, siendo

$$x = \cos.\frac{2k\pi}{n} + i\,\text{sen.}\frac{2k\pi}{n}\,,$$

una raiz de la ecuacion recíproca (2), como siempre se verifica la igualdad

$$\left(\cos.\frac{2k\pi}{n} + i\,\text{sen.}\frac{2k\pi}{n}\right) \times \left(\cos.\frac{2k\pi}{n} - i\,\text{sen.}\frac{2k\pi}{n}\right) = 1\,,$$

podemos establecer tambien esta otra:

$$\frac{1}{x} = \cos.\frac{2k\pi}{n} - i\,\text{sen.}\frac{2k\pi}{n}\,;$$

de donde resulta la expresion correspondiente á la (k),

$$x + \frac{1}{x} = y = 2\cos.\frac{2k\pi}{n}\,,$$

de las raices y de la ecuacion (3), en el supuesto de que reciba k sucesivamente los valores de la série numérica 1, 2..... $(n-1)$.

Pero cada par de estos valores, complementarios respecto de n, sustituidos por k en la expresion de y, producen el mismo para esta incógnita; y, por consecuencia, los valores diferentes de y, ó raices de la ecuacion (3), serán los $m = \frac{1}{2}(n-1)$ nada más que dicha ex-

presion produzca por la sustitucion en vez de k de los m primeros términos de la série entera 1, 2..... m.

Finalmente, si hacemos $y = 2z$, y dividimos despues por 2^m la ecuacion (3) se convierte en esta otra:

$$z^m + \frac{1}{2} z^{m-1} - \frac{1}{4}(m-1)z^{m-2} - \frac{1}{8}(m-2)z^{m-3} + \\ + \frac{1}{16}\frac{(m-2)\ (m-3)}{1.\ 2} z^{m-4} + \ldots\ldots = 0\ , \tag{4}$$

cuyas raices son los valores de la funcion trigonométrica

$$\cos.\frac{2k\pi}{n}, \quad \text{para} \quad k = 1,\ 2\ldots\ldots\ m,$$

entre ellos el mismo $\cos.\frac{2\pi}{n}$, y la cual debemos preferir siempre que nos propongamos determinar la funcion sencilla $\cos.\frac{2\pi}{n}$, y no la compleja $\cos.\frac{2\pi}{n} + i\,\text{sen.}\frac{2\pi}{n}$.

Ejemplos.—1.° De acuerdo con los principios establecidos anteriormente, la division de la circunferencia en *tres* partes iguales depende de la ecuacion de tercer grado

$$x^3 - 1 = 0.$$

Suprimiendo su raiz $x = 1$, y haciendo en el cociente resultante $x + \frac{1}{x} = y$, y despues $y = 2z$, segun dijimos, hallamos la siguiente (4):

$$z + \frac{1}{z} = 0\ :$$

cuya raiz $z = -\frac{1}{2}$ es igual á

$$\cos.\frac{2\pi}{3} = -\cos.\frac{\pi}{3} = -\operatorname{sen}.\frac{\pi}{6}.$$

Y, como $\operatorname{sen}.\frac{\pi}{6}$ es igual á la mitad de la cuerda del arco doble $\frac{2\pi}{6} = 60°$: y la cuerda de este arco es el lado del exágono, igual al radio, el valor de z es efectivamente el de $\cos.\frac{2k\pi}{3}$ para $k = 1$.

2.° La division de la circunferencia en *cinco* partes iguales, depende de la ecuacion

$$x^5 - 1 = 0:$$

de la cual, por el mismo procedimiento que antes, y teniendo presente que ahora es $n = 5 = 2.2 + 1$, $m = 2$, se deduce esta otra (4):

$$z^2 + \frac{1}{2}z - \frac{1}{4} = 0;$$

cuyas dos raices

$$\frac{-1+\sqrt{5}}{4} \quad \text{y} \quad \frac{-1-\sqrt{5}}{4}$$

deben ser iguales respectivamente á los valores de las funciones

$$\cos.\frac{2\pi}{5} \quad \text{y} \quad \cos.\frac{4\pi}{5}.$$

ó bien á los de estas otras:

$$\operatorname{sen}.\frac{\pi}{10} \quad \text{y} \quad -\operatorname{sen}.\frac{3\pi}{10}.$$

Y lo son efectivamente; puesto que

$$\text{sen.}\,\frac{\pi}{10} = \frac{1}{2}\ \text{cuerda}\left(\frac{2\pi}{10}\right),$$

ó igual á la mitad del lado del decágono inscrito ordinario, cuyo valor es

$$\frac{-1+\sqrt{5}}{2};$$

y la otra raiz

$$-\,\text{sen.}\,\frac{3\pi}{10} = \frac{1}{2}\cdot\frac{-1-\sqrt{5}}{2},$$

es la mitad del lado del decágono estrellado, cuyo lado vale

$$\frac{-1-\sqrt{5}}{2}.$$

Por este camino, y sin auxilio de las tablas trigonométricas, lograron resolver algebráicamente los antiguos geómetras hasta la ecuacion de grado *sétimo,* pero no la del *undécimo;* y aquí llegaban, cuando Gauss tomó el asunto por su cuenta, y le dió cima por el procedimiento que á continuacion explicaremos.

Ecuacion de la division del círculo.

Volvamos ahora á la expresion (k) de todas las raices de la ecuacion (1). Siempre que reciba k un valor primo con n, el correspondiente de la expresion mencionada,

$$r = \cos.\,\frac{2k\pi}{n} + i\,\text{sen.}\,\frac{2k\pi}{n},$$

representará una raiz propia (83) de la ecuacion (1); y las potencias sucesivas

$$r,\ r^2,\ r^3\ \ldots\ldots\ r^{n-1},\ r^n = 1, \qquad (r)$$

de dicha raiz, serán diferentes y expresarán todas las raices, propias y no propias, de aquella ecuacion (84), siendo el número de las propias $\varphi(n)$. Por lo tanto, segun la ley de la composicion de las ecuaciones, será:

$$x^n - 1 = (x - r)\left(x - r^2\right)\ldots\ldots\left(x - r^{n-1}\right)\left(x - r^n\right).$$

El segundo miembro de esta última puede distribuirse en grupos ó productos parciales, constituidos por los factores binomios correspondientes á las raices propias de las ecuaciones

$$x^D - 1 = 0 \qquad (1')$$

referidas á todos los divisores D, del número n. Designando por $f_D(x) = f(D)$ uno cualquiera de tales productos parciales, en cuyo supuesto la ecuacion $f(D) = 0$ contendrá exclusivamente las raices propias de la (1'), y por r' estas raices propias, dicho producto podrá escribirse en la forma explícita

$$f(D) = \Pi\,(x - r'),$$

con tal que el signo Π (producto) se extienda á todas las $\varphi(D)$ raices r'. Y, como todas las raices propias de las ecuaciones particulares (1') representan precisamente (82) todas las raices de la general (1), si D abraza todos los divisores de n, será tambien:

$$x^n - 1 = f(D')\,.\,f(D'')\,.\,f(D''')\ldots\ldots = \Pi f(D),$$

expresando D', D'', D'''..... todos aquellos divisores D, de n: descomposicion semejante á la del número n en sus factores primos.

Si hacemos sencillamente

$$x^n - 1 = F_n(x) = F(n) ,$$

la última igualdad se trasforma en la que sigue:

$$x^n - 1 = F(n) = \Pi f(D) ;$$

y de ésta se deduce (58) la inversa:

$$f_n(x) = f(n) = \frac{\Pi F(D_1)}{\Pi F(D_2)} = \frac{\Pi (x^{D_1} - 1)}{\Pi (x^{D_2} - 1)} . \qquad (5)$$

Esta última expresion, segun el modo como se ha formado, es una funcion de x con coeficientes racionales y enteros, de grado $\varphi(n)$, siendo igual á la unidad el de la mayor potencia de x; é, igualada á cero, representa, en efecto, la ecuacion cuyas raices son las propias y n^{as} de la unidad (83).

Si suponemos $n = p^{\pi}$, siendo p un número primo impar, tendremos:

$$f(p^{\pi}) = \frac{x^{p^{\pi}} - 1}{x^{p^{\pi-1}} - 1} = x^{p^{\pi-1}(p-1)} + x^{p^{\pi-1}(p-2)} + \ldots\ldots + \qquad (6)$$

$$+ x^{p^{\pi-1}} + 1 = 0 .$$

Y, por último, si hacemos $n = p$ simplemente, resulta:

$$f(p) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots\ldots + x + 1 = 0 , \qquad (7)$$

que es la ecuacion cuyas raices son las propias de la unidad (mod. p), ó, lo que es igual, todas las de la ecuacion binomia

$$x^p - 1 = 0,$$

con excepcion de la unidad misma; de manera que, si r significa una raiz de la ecuacion (7), todas ellas estarán representadas por las potencias

$$r,\ r^2,\ r^3 \ldots\ldots r^{p-1}.$$

Conclúyese de cuanto precede que el problema de la division de la circunferencia en un número primo impar, p, de partes iguales, puede considerarse como resuelto desde el momento en que nos sea conocida una raiz cualquiera de dicha ecuacion (7). Y esta ecuacion que, como la operacion material de dividir ó descomponer una circunferencia en cierto número de partes iguales, puede reducirse al caso más sencillo de ser primo semejante número, será la que en lo sucesivo designaremos con el nombre de *ecuacion de la division del círculo.*

Para resolverla necesitamos demostrar ante todo las leyes siguientes.

Relacion entre dos ecuaciones, siendo las raices de una de ellas las potencias p de las raices de la otra.

Sea una de las ecuaciones, con coeficientes enteros,

$$f(x) = x^m + a_1 x^{m-1} + a_2 x^{m-2} + \ldots\ldots + a_{m-1} x + a_m = 0, \qquad (1)$$

y sus raices correspondientes,

$$\alpha_1,\ \alpha_2,\ \alpha_3 \ldots\ldots \alpha_m.$$

Para formar ahora la otra ecuacion, cuyas raices fueran las potencias p (siendo p primo impar) de estas últimas, podríamos emplear

las fórmulas conocidas de Newton, por las cuales sabemos que se calculan las sumas de iguales potencias de las raices de una ecuacion en funcion de los coeficientes de la misma, ó inversamente estos coeficientes mediante aquellas sumas; mas no hace falta este cálculo expresivo, concretándonos puramente á determinar la relacion que enunciamos. En efecto, el Algebra enseña que, si z representa un número cualquiera, la ecuacion

$$x^m + a_1 z x^{m-1} + a_2 z^2 x^{m-2} + \ldots\ldots + a_{m-1} z^{m-1} x + a_m z^m = 0,$$

tiene por raices los productos por z de las raices de la ecuacion (1), á saber:

$$z\alpha_1, \quad z\alpha_2, \quad z\alpha_3 \ldots\ldots z\alpha_m.$$

Sustituyendo en esta última ecuacion por z sucesivamente las potencias

$$r, \quad r^2, \quad r^3 \ldots\ldots r^{p-1},$$

significando r lo que ha poco dijimos, formaríamos contando con la propuesta un sistema de p ecuaciones, cuyas raices, inclusas las de esta última, son respectivamente:

$$\begin{array}{llll}
\alpha_1, & \alpha_2, & \alpha_3 \ldots\ldots & \alpha_m \\
r\alpha_1, & r\alpha_2, & r\alpha_3 \ldots\ldots & r\alpha_m \\
r^2\alpha_1, & r^2\alpha_2, & r^2\alpha_3 \ldots\ldots & r^2\alpha_m \qquad (r) \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & \\
r^{p-1}\alpha_1, & r^{p-1}\alpha_2, & r^{p-1}\alpha_3 \ldots\ldots & r^{p-1}\alpha_m;
\end{array}$$

y cuyo producto $\Pi(x) = 0$ contendrá el sistema completo de estas raices.

Ahora bien, de la ecuacion evidente

$$(x-1)\,(x-r)\left(x-r^2\right) \ldots\ldots \left(x-r^{p-1}\right) = x^p - 1\,,$$

sustituyendo x por $\frac{x}{\alpha}$ y multiplicando despues por α^p, se deduce esta otra:

$$(x-\alpha)\,(x-r\alpha)\left(x-r^2\alpha\right) \ldots\ldots \left(x-r^{p-1}\alpha\right) = x^p - \alpha^p\,.$$

Y de esta forma general de los productos componentes del producto $\Pi(x)$, poniendo sucesivamente por α,

$$\alpha_1,\quad \alpha_2,\quad \alpha_3 \ldots\ldots \alpha_m\,,$$

la de este producto total:

$$\Pi(x) = \left(x^p - \alpha_1^{\,p}\right)\left(x^p - \alpha_2^{\,p}\right)\left(x^p - \alpha_3^{\,p}\right) \ldots\ldots \left(x^p - \alpha_m^{\,p}\right);$$

de la cual sencillamente, sustituyendo x^p por x, se obtiene la ecuacion

$$\left(x - \alpha_1^{\,p}\right)\left(x - \alpha_2^{\,p}\right)\left(x - \alpha_3^{\,p}\right) \ldots\ldots \left(x - \alpha_m^{\,p}\right) = 0\,,$$

cuyas raices son, en efecto, las potencias p de las raices de la (1).

Esta última ecuacion, despues de efectuadas las multiplicaciones que se indican en su primer miembro, la representamos por la que sigue, de forma semejante á la propuesta:

$$F(x) = x^m + b_1 x^{m-1} + b_2 x^{m-2} \ldots\ldots + b_{m-1} x + b_m = 0. \quad (2)$$

Para determinar ahora la relacion ó dependencia entre las ecuaciones (1) y (2), recordaremos (65) que los valores de las potencias

$$r,\quad r^2,\quad r^3 \ldots\ldots\ r^{p-1},$$

no cambian, aparte del órden, al sustituir por r cualquiera potencia r^e, cuyo esponente e sea primo con p; y, como el producto $\Pi(x)$ es una funcion simétrica de aquellas potencias, tampoco cambiará su valor aunque se permuten entre sí, ó se sustituya por r otra potencia cualquiera r^e. Al producto desarrollado $\Pi(x)$, y ordenado segun r, despues de haber rebajado los exponentes de esta letra ordenatriz superiores á p, bajo este módulo, podremos darle la forma:

$$\Pi(x) = \xi_0 + \xi_1 r + \xi_2 r^2 + \ldots\ldots + \xi_{p-1} r^{p-1} \qquad (r)$$

cuyos coeficientes ξ serán funciones enteras de x; de la cual, sustituyendo por r las potencias r^e, cuyos exponentes reciban sucesivamente los valores primos con p, $e = 2, 3 \ldots\ldots p-1$, se obtienen estas otras siempre de igual valor, como antes dijimos:

$$\Pi(x) = \xi_0 + \xi_1 r^2 + \xi_2 r^4 + \ldots\ldots + \xi_{p-1} r^{2(p-1)} \qquad (r^2)$$

. . . . . .

. . . . . .

$$\Pi(x) = \xi_0 + \xi_1 r^{p-1} + \xi_2 r^{2(p-1)} + \ldots\ldots + \xi_{p-1} r^{(p-1)(p-1)} \qquad (r^{p-1})$$

Sumando ordenadamente los valores, diferentes en forma, del producto $\Pi(x)$, expresados por las igualdades (r), $(r^2) \ldots\ldots (r^{p-1})$, resulta la siguiente:

$$(p-1)\,\Pi(x) = (p-1)\,\xi_0 + \xi_1\left(r + r^2 + r^3 + \ldots\ldots + r^{p-1}\right) +$$

$$\ldots\ldots\ldots + \xi_2\left(r^2 + r^4 + \ldots\ldots + r^{2(p-1)}\right) +$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$+ \xi_{p-1}\left(r^{p-1} + r^{2(p-1)} + \ldots\ldots + r^{(p-1)(p-1)}\right)$$

y, teniendo en cuenta que las sumas, inclusas en los paréntesis, que multiplican á ξ_1, ξ_2 ..... ξ_{p-1}, tienen todas por valor -1 (88), esta otra:

$$(p-1)\,\Pi(x) = p\,\xi_0 - \left(\xi_0 + \xi_1 + \xi_2 + \ldots\ldots + \xi_{p-1}\right).$$

Mas las cantidades ξ se obtienen todas del producto $\Pi(x)$, haciendo en él $r = 1$; y, como en esta suposicion todas las ecuaciones, que figuraban como factores distintos del mismo, se igualan á la propuesta $f(x)$, dicho producto se convertirá en la potencia $f(x)^p$, y la última ecuacion en la congruencia

$$\Pi(x) \equiv f(x)^p \pmod{p}.$$

Sustituyendo por $f(x)$ su polinomio equivalente (1), y elevando éste á la potencia p, tendremos (66):

$$\Pi(x) \equiv x^{mp} + a_1^p \cdot x^{(m-1)p} + a_2^p \cdot x^{(m-2)p} + \ldots\ldots +$$

$$+ a_{m-1}^p \cdot x^p + a_m^p \pmod{p}$$

ó bien, aplicando la congruencia (A) del artículo (66) antes citado;

$$\Pi(x) \equiv x^{mp} + a_1 x^{(m-1)p} + a_2 x^{(m-2)p} + \ldots\ldots$$

$$+ a_{m-1} x^p + a_m \text{ (mod. } p\text{)}.$$

y, por consecuencia, evidentemente:

$$f(x)^p \equiv f(x^p) \text{ (mod. } p\text{)} \qquad (3)$$

Pero, si reemplazamos x^p por x, el primer miembro de la penúltima congruencia, ó el producto $\Pi(x)$, se convierte en el de la ecuacion (2), $F(x)$; y el segundo en $f(x)$; y, por lo tanto, será tambien

$$F(x) \equiv f(x) \text{ (mod. } p\text{)}: \qquad (4)$$

relacion que buscamos, y que en lenguaje vulgar se expresa del modo siguiente:

Siempre que p sea un número primo superior á 2, la ecuacion, $F(x) = 0$, *cuyas raices son las potencias p de las de otra ecuacion* $f(x) = 0$, *es congruente con ésta última, segun el módulo p.*

125.—*La ecuacion de la division del círculo es irreducible.*

Llámase *irreducible* toda funcion $f(x)$, entera y con coeficientes racionales, que no puede descomponerse en factores con coeficientes tambien racionales. Siendo la funcion $f(x)$ irreducible, la ecuacion $f(x) = 0$, toma el mismo nombre.

Teorema fundamental.—Una ecuacion irreducible, $f(x) = 0$, *no puede tener ninguna raiz comun con otra ecuacion,* $F(x) = 0$, *de menor grado y coeficientes racionales.* Pues, si las ecuaciones $f(x) = 0$, y $F(x) = 0$, tuvieran una raiz comun, sus primeros miembros tendrian un máximo comun divisor (80), de grado inferior á $f(x)$, y con coefi-

cientes tambien racionales; y, por consecuencia, $f(x)$ un factor racional, contra lo supuesto.

Corolario.—Si la ecuacion irreducible $f(x) = 0$, *tiene una raiz comun con otra ecuacion de coeficientes tambien racionales* $F(x) = 0$, *todas las raices de la primera satisfarán á la segunda, ó ésta, en otro caso, será idéntica* (67) (*). Desde luego sucederá esto último, segun el teorema, siempre que la funcion $F(x)$ sea de grado inferior á $f(x)$. Admitamos, pues, que $F(x)$ no sea de grado inferior á $f(x)$, y dividamos una funcion por otra; representando por $C(x)$ el cociente y por $R(x)$ el resto correspondiente, tendremos:

$$F(x) = f(x)\, C(x) + R(x).$$

Toda raiz x que satisfaga á las ecuaciones $F(x) = 0$, y $f(x) = 0$, satisfará tambien á la ecuacion $R(x) = 0$; y, como esta última es de grado inferior á $f(x) = 0$, segun ántes digimos, será idéntica con cero. Suprimiéndola, por lo tanto, de la igualdad arriba escrita resulta esta otra:

$$F(x) = f(x) \,.\, C(x):$$

la cual manifiesta que todas las raices de la ecuacion $f(x) = 0$, satisfacen tambien á la ecuacion $F(x) = 0$, que es lo que pretendíamos demostrar:

Una ecuacion $f(x) = 0$, con coeficientes enteros, é igual á la unidad el de la mayor potencia de la incógnita, será irreducible siempre que su primer miembro no pueda ser descompuesto en factores con coeficientes tambien enteros (76).

a) — Supongamos ahora que la funcion

$$X = x^{p^{\pi-1}(p-1)} + x^{p^{\pi-1}(p-2)} + \ldots\ldots + x^{p^{\pi-1}} + 1 = 0 \qquad (1)$$

que comprende como caso particular la (6), no sea irreducible, sino resoluble, por el contrario, en el producto de dos funciones enteras con

(*) Serret, *Cours d' Algèbre supérieure*, 3.ª ed., §. 100.

coeficientes enteros, $\varphi(x)$ y $\psi(x)$: podremos establecer la igualdad

$$X = \varphi(x).\psi(x):$$

la cual, en la hipótesis de ser $x = 1$, se convierte en esta otra:

$$p = \varphi(1).\psi(1):$$

de donde se infiere que uno de los dos factores del segundo miembro, $\varphi(1)$, por ejemplo, debe ser igual á ± 1.

Designando por r una raiz propia cualquiera de la ecuacion $x^{p^{\pi}} = 1$, la série de potencias

$$r,\ r^{\alpha},\ r^{\beta} \ldots\ldots r^{\gamma},$$

cuyos exponentes representan los números primos con p^{π} é inferiores á este número, comprende todas las raices propias y de grado p^{π} de la unidad, esto es: todas las raices de la ecuacion (1), entre las cuales se hallarán necesariamente las que satisfacen á la ecuacion $\varphi(x) = 0$, factor de aquella; por cuya razon será cierta siempre la igualdad

$$\varphi(r).\varphi(r^{\alpha}).\varphi(r^{\beta}) \ldots\ldots \varphi(r^{\gamma}) = 0$$

Y esto prueba que el producto

$$\varphi(x).\varphi(x^{\alpha}).\varphi(x^{\beta}) \ldots\ldots \varphi(x^{\gamma})$$

se convierte en cero, cuando en él se sustituyen por x todas las $p^{\pi-1}(p-1)$ raices r de la ecuacion (1), y que es divisible, por consecuencia, por el primer miembro, X, de esta ecuacion. De donde se desprende que

$$\varphi(x).\varphi(x^{\alpha}).\varphi(x^{\beta}) \ldots\ldots \varphi(x^{\gamma}) = X.Q(x),$$

cuando el cociente $C(x)$ designa una funcion entera, con coeficientes enteros, de x. Si en esta igualdad hacemos $x = 1$, como el número de factores de su primer miembro es $p^{\pi-1}(p-1)$, resulta la siguiente:

$$\varphi(1)^{p^{\pi-1}(p-1)} = p.C(1)$$

ó bien:

$$1 = p.C(1)$$

que expresa el absurdo de ser la unidad divisible por el número p. Y de este absurdo, retrocediendo, se concluye que es inadmisible la descomposicion supuesta del primer miembro de la ecuacion (1), y, por lo tanto, que ésta es irreducible.

b) — Demostrado que la ecuacion $f_n(x) = 0$, cuyas raices son las primitivas y n^{as} de la unidad, es irreducible para $n = p^{\pi}$, vamos á demostrar ahora que, si dicha ecuacion se supone irreducible para un número n', compuesto de k factores primos diferentes, lo será tambien para otro número n que contenga un factor primo más; en cuyo caso quedará demostrado que la ecuacion $f_n(x) = 0$, es irreducible para cualquier número n.

Hagamos, pues, $n = p^{\pi}.n'$, constando n' de k factores primos, diferentes del factor p; y admitamos, por de pronto, que sea

$$f_n(x) = \varphi(x).\psi(x); \qquad (1)$$

y

$$\Phi(x) = 0, \qquad \Psi(x) = 0$$

las ecuaciones cuyas raices sean las potencias de grado p^{π} de las raices de las ecuaciones

$$\varphi(x) = 0, \qquad \psi(x) = 0$$

respectivamente. Aplicando π veces la ley (124), tendremos las congruencias:

$$\varphi(x) \equiv \Phi(x) \qquad \psi(x) \equiv \Psi(x) \pmod{p}. \qquad (2)$$

Sean ahora: r una raiz propia de grado n de la unidad, y ρ y ω otras raices propias de la unidad, pero de los grados p^{π} y n'; y tendremos (85) tambien: $r = \rho \,.\, \omega$; de donde $p^{p^{\pi}} = \omega^{p^{\pi}}$. Y, como p^{π} es primo con n', será asimismo (84) $r^{p^{\pi}}$ igual á una raiz propia, ω', de la unidad, de grado n'. De lo cual se deduce que, si r designa sucesivamente cada una de las raices de las ecuaciones $\varphi(x) = 0$, y $\psi(x) = 0$, en cuyo caso la potencia correspondiente $r^{p^{\pi}}$ será una raiz de la ecuacion $\Phi(x) = 0$, ó de la $\Psi(x) = 0$, estas últimas habrán de tener alguna raiz, comun con la

$$f_{n'}(x) = f(n') = 0. \qquad (3)$$

Y, como ésta es irreducible, aquellas deberán quedar satisfechas por todas las raices de la misma, entre las cuales se encuentra la ω que antes dijimos: por cuyo motivo de las congruencias (2) se desprenden estas otras:

$$\varphi(\omega) \equiv 0, \qquad \psi(\omega) \equiv 0 \ (\text{mod. } p).$$

Con lo cual la ecuacion (1) se convierte en la siguiente:

$$f_n(\omega) = p^2 \,.\, F(\omega); \qquad (4)$$

representando $F(\omega)$ una funcion entera de ω.

Por otra parte, de las ecuaciones

$$x^n - 1 = \Pi f(D), \qquad x^{n:p} - 1 = \Pi f(\Delta),$$

en las cuales D y Δ representan todos los divisores de n y de $n:p$, respectivamente, estando, por lo tanto, los Δ comprendidos entre los D, y entre los D exclusivamente el $D = n$, se deduce que el cociente de sus primeros miembros,

$$\frac{x^{n}-1}{x^{n:p}-1},$$

es una funcion entera, divisible por $f_{n}(x)$: esto es que

$$\frac{x^{n}-1}{x^{n:p}-1} = f_{n}(x) \,.\, C(x):$$

siendo $C(x)$ entera. Y, si en esta ecuacion hacemos $x = \omega$, teniendo en cuenta que $n = p^{\pi} \,.\, n'$, $n : p = p^{\pi-1} \,.\, n'$, y $\omega^{n'} = 1$, resulta la igualdad:

$$p = f_{n}(\omega) \,.\, C(\omega);$$

que, en combinacion con la (4), produce la siguiente:

$$1 = p \,.\, F(\omega) \,.\, C(\omega).$$

Suprimiendo del producto desarrollado $F(\omega) \,.\, C(\omega)$, en virtud de la ecuacion idéntica $f_{n'}(\omega) = 0$, de grado $\varphi(n')$, todas las potencias de ω, superiores á la $\varphi(n') - 1$, hallaremos una ecuacion de la forma

$$1 = p\left(a_{0} + a'_{1}\omega + a_{2}\pi^{2} + \ldots\ldots + a_{\varphi(n')-1}\omega^{\varphi(n')-1}\right);$$

y de ésta que, por haber supuesto irreducible la ecuacion (3), debe ser idéntica, el absurdo

$$1 = p\,a_{0}:$$

del cual se desprende que tambien lo es la descomposicion supuesta en la igualdad (1); y, por último, que la funcion $f(n)$, es irreducible.

c—) *Kronecker*, á quien se debe la sencilla demostracion (*a*) que dejamos transcrita, y sobre la cual se funda la (*b*) de *Arndt*, publicó otra (*) además para el caso general, como corolario de una propiedad de la funcion, $f(n)$, segun la cual, no solo es ésta irreducible en el sentido estricto de la palabra, sino tambien en otro más amplio, é interesante para nosotros, como en adelante veremos. Concretándonos, pues, á la ecuacion que llamamos de la division del círculo (123), vamos á demostrar en primer término que goza de la propiedad mencionada, como se expresa en la proposicion siguiente; y, en consecuencia, que es asimismo irreducible, conforme con la definicion de esta palabra.

La funcion

$$X = x^{p-1} + x^{p-2} + \ldots\ldots + x + 1$$

no puede descomponerse en factores cuyos coeficientes sean funciones racionales y enteras de una raiz α *de la ecuacion irreducible* $f_e(x)$, *siendo* $p - 1 = e.f.$

Como lema indispensable probaremos que toda funcion racional de α puede ser expresada bajo la forma

$$\frac{a_0 + a_1\alpha + \ldots\ldots + a_{\varepsilon-1}\alpha^{\varepsilon-1}}{m}$$

en la cual es $\varepsilon = \varphi(e)$, y los coeficientes a no tienen todos con m un mismo factor comun. En efecto, la funcion racional $\frac{F(\alpha)}{\varphi(\alpha)}$ cuyos dos términos son funciones enteras de α, designando por $\alpha', \alpha'' \ldots\ldots \alpha^{(\varepsilon-1)}$ las otras raices de la ecuacion $f(e) = 0$, puede tambien escribirse de este modo:

(*) J. de Liouville, t. 19, pág. 183. Otra demostracion dió Serret. J. de Liouville, t. 15, pág. 296.

$$\frac{F(\alpha)\,.\,\varphi(\alpha')\,\varphi(\alpha'')\,.....\,\varphi\left(\alpha^{(\varepsilon-1)}\right)}{\varphi(\alpha)\,.\,\varphi(\alpha')\,\varphi(\alpha'')\,.....\,\varphi\left(\alpha^{(\varepsilon-1)}\right)}.$$

El denominador de esta nueva forma, como funcion simétrica de todas las raices propias de grado e de la unidad, es tambien funcion entera de los coeficientes de la ecuacion $f(e)=0$, y, por consecuencia, igual á un número entero, m; y el producto $\varphi(\alpha')\,\varphi(\alpha'')\,.....\,\varphi\left(\alpha^{(\varepsilon-1)}\right)$ que figura en el numerador, y áun todo éste, es una funcion entera de α, cuyo grado, por medio de la ecuacion idéntica $f_e(\alpha)=0$ de grado $\varphi(e)=\varepsilon$, se hace menor que e: la cual puede, por lo tanto, reducirse á la forma $a_0+a_1\alpha+.....+a_{\varepsilon-1}\alpha^{\varepsilon-1}$; y, como cualquier factor, comun á m y todos los coeficientes a, puede suprimirse, la forma de toda funcion racional de α será efectivamente la que en un principio escribimos (*).

Dicho esto, supongamos que la funcion X es descomponible en los factores $\varphi(x)$ y $\psi(x)$, cuyos coeficientes racionales dependan de α: de la ecuacion correspondiente

$$X=\varphi(x)\,.\,\psi(x), \qquad (1)$$

haciendo $x=1$, resulta esta otra:

$$p=\varphi(1)\,.\,\psi(1): \qquad (2)$$

en la cual $\varphi(1)$ y $\psi(1)$ serán evidentemente funciones racionales y enteras de α. Escribiendo estas funciones bajo la forma antes expresada, tendremos:

(*) Véase tambien Lagrange, *Traité de la R. des équations numériques. Note IV*, 1808.

$$\varphi(1) = \frac{a_0 + a_1 \alpha + \ldots\ldots + a_{\varepsilon-1} \alpha^{\varepsilon-1}}{m} = \frac{A(\alpha)}{m}$$

$$\psi(1) = \frac{b_0 + b_1 \alpha + \ldots\ldots + b_{\varepsilon-1} \alpha^{\varepsilon-1}}{n} = \frac{B(\alpha)}{n} \qquad (3)$$

con lo cual se convierte la ecuacion (2) en la siguiente:

$$p \,.\, mn = A(\alpha) \,.\, B(\alpha).$$

Esta indica que sólo en una de las dos funciones, $A(\alpha)$, $B(\alpha)$, pueden ser todos los coeficientes divisibles por p; pues, si se verificaran, por el contrario, las igualdades

$$A(\alpha) = p \,.\, C(\alpha), \qquad B(\alpha) = p \,.\, D(\alpha), \qquad (4)$$

siendo $C(\alpha)$ y $D(\alpha)$ funciones enteras con coeficientes enteros de α, resultaria: por una parte, segun las condiciones de los coeficientes a y b de las formas (3), que ni m ni n serian divisibles por p; y, por otra, la igualdad

$$mn = p \,.\, C(\alpha) \,.\, D(\alpha)$$

que, mediante la ecuacion idéntica $f_e(\alpha) = 0$, puede reducirse á la forma

$$mn = p\left(c_0 + c_1 \alpha + \ldots\ldots + c_{\varepsilon-1} \alpha^{\varepsilon-1}\right);$$

y de ésta, al fin, la consecuencia imposible $mn = p\,c_0$; porque ni m, ni n son, como antes dijimos, divisibles por p.

Vamos á demostrar ahora, inversamente, que las igualdades (4) son consecuencia necesaria de la supuesta descomposicion (1) de X.

Designando por r una raiz de la ecuacion $X = 0$, esto es, una raiz

propia de grado p de la unidad, los factores $\psi(x)$ y $\psi(x)$ de X podrán escribirse bajo las formas (ordinarias tambien como la de X):

$$\varphi(x) = \left(x - r^{h'}\right)\left(x - r^{h''}\right)\left(x - r^{h'''}\right) \ldots\ldots$$

$$\psi(x) = \left(x - r^{i'}\right)\left(x - r^{i''}\right)\left(x - r^{i'''}\right) \ldots\ldots$$

donde las h y las i representan números primos con p. Fijándonos en la primera solamente, y haciendo en ella $x = 1$, será:

$$\varphi(1) = \left(1 - r^{h'}\right)\left(1 - r^{h''}\right)\left(1 - r^{h'''}\right) \ldots\ldots$$

y así se ve claro que $\varphi(1)$ consta de factores de la forma $\left(1 - r^{h}\right)$. Si elevamos esta forma general á la potencia p, como p es impar y $r^{p} = 1$, los dos términos extremos del desarrollo de $\left(1 - r^{h}\right)^{p}$ se destruyen; y todos los restantes son divisibles por p; y la última igualdad, elevada á la potencia p, afectará, en consecuencia, la forma

$$\varphi(1)^{p} = p \,.\, F(r), \qquad (5)$$

siendo $F(r)$ funcion entera de r. Ahora bien, ordenando segun las potencias de z, el producto efectuado

$$\left[z - p \,.\, F(r)\right]\left[z - p \,.\, F(r^{2})\right] \ldots\ldots \left[z - p \,.\, F(r^{p})\right],$$

se advertirá que el coeficiente del primer término z^{p}, máxima potencia de z, será la unidad; y que los de los otros términos son funciones simétricas de las raices $r, r^{2}, \ldots\ldots r^{p}$, de la ecuacion $x^{p} = 1$, multiplicadas por las diversas potencias de p; por lo cual no hay dificultad en escribir el desarrollo de tal producto sencillamente como sigue:

$$z^{p} - p \,.\, G(z),$$

representando $G(z)$ una funcion entera de z. Mas este producto desaparece, en virtud de la ecuacion (5), sustituyendo en él por z el valor (3)

$$\varphi(1)^{p} = \frac{A(\alpha)^{p}}{m^{\mu}};$$

y entónces resulta la igualdad:

$$A(\alpha)^{p^{2}} = p \,.\, H(\alpha); \qquad (6)$$

en la cual $H(\alpha)$ es una funcion entera con coeficientes enteros de α. Y, como además, por ser $p = ef + 1$, y, de consiguiente, $\alpha^{p} = \alpha$, tenemos (124):

$$A(\alpha)^{p} \equiv A(\alpha) \,(\text{mod. } p)$$

y tambien

$$A(\alpha)^{p^{2}} \equiv A(\alpha) \quad \text{ó} \quad A(\alpha)^{p^{2}} = A(\alpha) + p \,.\, H'(\alpha),$$

siendo $H'(\alpha)$ funcion entera y con coeficientes enteros de α, conclúyese que la igualdad (6) expresa lo mismo que la primera de las ecuaciones (4). Igual resultado puede hallarse para la segunda; y así finalmente deducirse que la supuesta descomposicion de X, que conduce á las igualdades contradictorias (4), no es posible.

MÉTODO DE GAUSS PARA RESOLVER LA ECUACION DEL CÍRCULO.

126.—*Sus fundamentos.*

Este modo de resolver la ecuacion del círculo consiste en descomponer la funcion X en factores, gradualmente, y de tal manera que los coeficientes de estos factores puedan ser determinados por ecuaciones

del menor grado posible, hasta llegar así á los factores simples, ó á las raices mismas de dicha ecuacion.

Manifestaremos, dice Gauss (*), que, si descomponemos el número $(p-1)$ en factores, $a, b, c, \ldots$ (y éstos pueden ser simples), la funcion X puede, desde luego, resolverse en a factores del grado $(p-1):a$, cuyos coeficientes se determinan por una ecuacion del grado a; despues, cada uno de estos factores en otros b del grado $(p-1):ab$, con el auxilio de una ecuacion del grado b; y, en conclusion, que designando por m el número de los factores, $a, b, c, \ldots$, la resolucion de la ecuacion $X=0$, se convierte en la de m ecuaciones de los grados $a, b, c \ldots$ respectivamente. Pero todas estas descomposiciones graduales son posibles únicamente á condicion de que la ecuacion del círculo pertenezca á la clase de las que llamó Kronecker *abelianas*, por haber sido *Abel* quien demostró primero, generalizando el procedimiento de Gauss, que, si dos raices de una ecuacion *irreducible* se hallan sometidas á la ley de ser una de ellas funcion racional de la otra, la resolucion de aquella puede convertirse en la de otras ecuaciones de grados inferiores.

Que la ecuacion del círculo es irreducible lo hemos demostrado anteriormente: veamos ahora cuál es la dependencia establecida por Gauss entre sus raices, necesaria y suficiente para calificarla de abeliana. Sabemos que, si r significa una raiz cualquiera de la ecuacion del círculo,

$$X = x^{p-1} + x^{p-2} + \ldots + x + 1 = 0, \qquad (1)$$

todas ellas están representadas por la serie de potencias

$$r, r^2, r^3, \ldots r^{p-1}. \qquad (2)$$

Gauss tuvo la feliz idea de sustituir la progresion aritmética

$$1, 2, 3 \ldots (p-1)$$

por la geométrica,

(*) D. A., §. 342.

$$1 , g , g^2 \ldots\ldots g^{p-2} \qquad (3)$$

cuyos términos, fuera del órden, son congruentes (mod. p) con los de aquella, siendo g, como sabemos (85), una raiz primitiva del número primo p. Mediante dicha sustitucion las raices (2) pueden ser escritas en el órden siguiente:

$$r , r^g , r^{g^2} \ldots\ldots r^{g^{p-2}} \qquad (4)$$

Así colocadas, fácilmente se percibe que cada una de ellas es la potencia g de la precedente. Y lo mismo sucede colocándolas en círculo, cualquiera que sea la que se tome para punto de partida; pues de la congruencia $g^{p-1} \equiv 1$, que define la raiz primitiva g, del número p, se deducen las relaciones: $\left(r^{g^{p-2}}\right)^g = r^{g^{p-1}} \equiv r (\text{mod. } p)$: las cuales evidencian que la primera raiz de la serie (4) es asimismo la potencia g de la última. Bajo el uno ó el otro modo de expresarlas, podemos afirmar, por último, que *cada una de las raices de la ecuacion del círculo es la misma funcion racional de la precedente.*

127.—*Reduccion de las funciones de las raices de la ecuacion del círculo á su forma normal.*

Ante todo recordaremos que la resolucion algebráica de las ecuaciones estriba en la posibilidad de formar ciertas funciones enteras de sus raices, funciones cuyos valores podamos determinar por ecuaciones de menor grado ó mas fáciles de manejar que la propuesta, y de los cuales se deduzcan inmediatamente los valores de las raices de ésta. Con tales antecedentes se comprende bien que las funciones de que vamos á tratar ahora ejerzan una influencia excepcional en la resolucion de la ecuacion del círculo.

Sea

$$F(r, r^2, \ldots\ldots r^{p-1})$$

una funcion entera, cualquiera, de las raices de dicha ecuacion. Y, por serlo de todas, puede naturalmente considerarse como funcion de una sola de ellas, y escribirse bajo la forma:

$$f(r) = a_0 + a_1 r + a_2 r^2 + \ldots\ldots + a_m r^m :$$

ó, bien, reemplazando los exponentes de r por sus restos mínimos (mod. p), en la siguiente:

$$f(r) = b_0 + b_1 r + b_2 r^2 + \ldots\ldots + b_{p-1} . r^{p-1} :$$

cuyos coeficientes serán funciones enteras de los que figuran en la funcion dada, F, y, por consecuencia, racionales y enteros, segun y como los de la funcion propuesta lo sean. Sustituyendo x por r en la ecuacion del círculo, multiplicándola despues por b_0, y restando el producto resultante de la ecuacion última, se obtiene la expresion

$$A_1 r + A_2 r^2 + \ldots\ldots + A_{p-1} r^{p-1} \qquad (5)$$

Siempre que los coeficientes de la funcion dada sean números racionales, ó, más generalmente, funciones racionales y enteras de una raiz α, de la ecuacion binomia $x^{p-1} = 1$, la $f(r)$ se hallará completamente determinada por la forma (5): y hé aquí la razon de llamarla forma *normal*.

Para la funcion $f(r)$, no puede existir otra forma normal, diferente de la expresada; pues, suponiendo que existiera y fuese la siguiente:

$$B_1 r + B_2 r^2 + \ldots\ldots + B_{p-1} r^{p-1}, \qquad (5')$$

restándolas una de otra, y dividiendo su diferencia por r, se obtendria la ecuacion del grado $p-2$,

$$A_1 - B_1 + \left(A_2 - B_2\right) r + \ldots\ldots + \left(A_{p-1} - B_{p-1}\right) r^{p-2} = 0:$$

cuyos coeficientes, que habrian de ser números racionales ó funciones racionales de α, se reducirian todos á cero, por ser irreducible la ecuacion del círculo (1) en el sentido lato que demostramos (125—*c*): y, en conclusion, las dos formas (5) y (5') coincidirian.

Fuera ya de duda la completa determinacion de la funcion $f(r)$ de las raices de la ecuacion del círculo, ó de la unidad, bajo su forma normal, tal y como la hemos constituido, debemos advertir, para armonizarla con la expresion dada por Gauss á dichas raices, que los exponentes de r que figuran en la misma es preciso reemplazarlos por la série (3) de las potencias de g. La forma (5), por efecto de tal sustitucion, se convierte en la siguiente:

$$f(r) = a_0\, r + a_1\, r^{g} + a_2\, r^{g^2} + \ldots\ldots + a_{p-2}\, r^{g^{p-2}} \qquad (6)$$

Acerca de la relacion entre los coeficientes de las dos formas (5) y (6), basta notar que, siempre que se verifique la congruencia $h \equiv g^k$ (mod. p), las potencias r^h y r^{g^k} serán iguales, y tambien sus coeficientes correspondientes A_h y a_k en una y otra forma; y, como $k = \text{ind. } h$, será: $A_h = a_k = a_{\text{ind } h}$.

Conclúyese de todo lo dicho que: *una funcion entera, cualquiera que sea, de las raices de la ecuacion del círculo, puede reducirse á otra funcion entera de una sola raiz de aquella ecuacion bajo su forma normal, cuyos coeficientes serán tambien funciones enteras de los coeficientes dados.*

128.—*Distribucion en períodos de las raices de la ecuacion del círculo.*

Si descomponemos en dos factores cualesquiera $p-1 = ef$, las raices de la ecuacion del círculo, podrán expresarse como sigue:

$$r^{g^0}, r^{g^1}, r^{g^2} \ldots\ldots r^{g^{e-1}}, r^{g^e}, r^{g^{e+1}}, \ldots\ldots r^{g^{2e-1}},$$

$$r^{g^{2e}}, r^{g^{2e+1}}, \ldots\ldots r^{g^{3e-1}}, r^{g^{3e}} \ldots\ldots\ldots\ldots\ldots$$

$$r^{g^{(f-1)e}}, r^{g^{(f-1)e+1}}, \ldots\ldots r^{g^{fe-1}} = r^{g^{p-2}}.$$

Cada una de estas raices es, segun sabemos, la potencia g de la anterior; pero no hay inconveniente tampoco en distribuirlas en e grupos de f términos, con la condicion de que cualquiera de estos sea, no ya la potencia g, sino la potencia g^e del precedente. Representando para mayor sencillez por $[\lambda]$ la potencia r^λ, y entónces $[0]=1$, $[\lambda].[\mu]=[\lambda+\mu]$, $[\lambda]^\mu=[\lambda\mu]$, los e grupos mencionados, indicada la suma de los f términos correspondientes á cada uno, figuran en el adjunto cuadro:

$$\eta_0 = [g^0] + [g^e] + [g^{2e}] + \ldots\ldots + [g^{(f-1)e}]$$

$$\eta_1 = [g^1] + [g^{e+1}] + [g^{2e+1}] + \ldots\ldots + [g^{(f-1)e+1}]$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\eta_{e-1} = [g^{e-1}] + [g^{2e-1}] + [g^{3e-1}] + \ldots\ldots + [g^{fe-1}]$$

Estas sumas, que desempeñan el papel más importante para resolver el problema que estamos estudiando, se llaman *períodos f-membres*, y sus principales propiedades son las siguientes:

1. *Los períodos definidos permanecen invariables cuando se sustituye en ellos la raiz* $r=[1]$ *por cualquiera de los términos del primero,* η_0 ; *y se permutan circularmente, si por la raiz* r *se pone otra perteneciente á uno de los demás períodos.* En efecto, sea el período

$$\eta_k=[g^k]+[g^{e+k}]+\ldots\ldots[g^{(f-2)e+k}]+[g^{(f-1)e+k}]$$

cuyo término general tiene la forma

$$[g^{me+k}].$$

Es claro que reemplazar en él r por r^{g^e} equivale á multiplicar los exponentes $g^k, g^{e+k}\ldots\ldots$ por g^e, y el nuevo período que de esta operacion resulta,

$$[g^{e+k}]+[g^{2e+k}]\ldots\ldots[g^{(f-1)e+k}]+[g^k],$$

no difiere del anterior η_k. Esto prueba tambien que, en el caso de que los índices de los períodos η_k excedan de $e-1$, siempre serán iguales aquellos cuyos índices sean congruentes (mod. e); esto es: $\eta_k=\eta_{k'}$ si $k\equiv k'$ (mod. e): lo cual no debe olvidarse.

Pero, si en lugar de sustituir r por r^{g^e}, ó bien por $r^{g^{me}}$, sustituyéramos r por r^{g^k}, el término general del período η_k, antes escrito, se transformaria en el siguiente:

$$[g^{me+k+k}];$$

el período η_k, por consecuencia, se convertiria en el η_{k+k}, y los períodos

$$\eta_0, \eta_1, \eta_2 \ldots\ldots \eta_{e-1}, \text{ en los } \eta_h, \eta_{h+1}, \ldots\ldots \eta_{h+e-1},$$

ó en estos otros:

$$\eta_h, \eta_{h+1} \ldots\ldots \eta_{e-1}; \eta_0, \eta_1, \ldots\ldots \eta_{h-1} \text{ etc.:}$$

lo cual quiere decir que la sustitucion supuesta produce el cambio en h lugares de cada uno de los períodos η_i, ó, en otros términos, la permutacion *circular* de los mismos.

2.ª *La distribucion en períodos de las raices de la ecuacion del círculo es independiente de la raiz primitiva de p, que se elija para representarlas.*—Sea G otra raiz primitiva de p; entre ésta y la g antes usada habrá de verificarse necesariamente (85) la congruencia

$$G \equiv g^h \pmod{p}$$

á condicion de que el exponente h sea primo con $p-1$, y, de consiguiente, con cada uno de los factores, e y f, de este número. Si designamos por $\varepsilon_0, \varepsilon_1 \ldots\ldots \varepsilon_{e-1}$, los períodos correspondientes á la nueva raiz G, tendremos:

$$\varepsilon_0 = [g^0] + [g^{he}] + [g^{2he}] + \ldots\ldots + [g^{(f-1)he}].$$

La série de los exponentes que figuran en este período,

$$0, he, 2he, \ldots\ldots (f-1)he$$

es (63) congruente, aparte del órden, segun el módulo $(p-1)$, con la de los de η_0,

$$0, e, 2e, \ldots\ldots (f-1)e;$$

de lo cual se deduce que $\varepsilon_0 = \eta_0$; y del mismo modo se demostraria

que son ciertas las igualdades: $\varepsilon_1 = \eta_h$, $\varepsilon_2 = \eta_{2h}$ ..... $\varepsilon_{e-1} = \eta_{(e-1)h}$. Pero tambien, por ser h primo con e, la série de los números

$$0,\ h,\ 2h,\ \ldots\ldots (e-1)h,$$

es congruente (mod. e), prescindiendo del órden, con esta otra:

$$0,\ 1,\ 2\ldots\ldots (e-1):$$

luego los nuevos períodos $\varepsilon_0, \varepsilon_1 \ldots\ldots \varepsilon_{e-1}$ coinciden, fuera del órden, con los antiguos $\eta_0, \eta_1 \ldots\ldots \eta_{e-1}$. Nótese, sin embargo, que un período cualquiera, η_h, por ejemplo, no es lo mismo referido á g que á G; sino que sus elementos se convierten, por el contrario, en los del período η_{k+h} cuando se sustituye la raiz primitiva g, base del primero, por la G á que se refiere el segundo; produciendo tal sustitucion de raices, h permutaciones circulares, segun antes indicamos, en la série de los períodos η.

3.ª *Los e períodos difieren numéricamente unos de otros.*— En efecto: admitamos, por el contrario, que los dos períodos η_h y η_k, cuyos índices son menores que e, sean iguales, esto es: que se verifique la ecuacion:

$$[g^h] + [g^{h+e}] + \ldots\ldots + [g^{h+(f-1)e}] =$$

$$[g^k] + [g^{k+e}] + \ldots\ldots + [g^{k+(f-1)e}].$$

Desde luego podemos asegurar que esta ecuacion no es idéntica, porque á diferentes períodos corresponden tambien raices diferentes de la unidad. Ahora bien, si reemplazamos los exponentes de r que en dicha ecuacion figuran por sus restos mínimos (mod. p), y dividimos luego por r, operacion posible por no ser igual á la unidad ninguna de las potencias de r, resultará una ecuacion, no idéntica, del grado

$p-2$ á lo sumo, que tendrá una raiz r, comun con la irreducible del círculo que es del grado $p-1$; y no siendo este resultado posible, tampoco puede serlo la igualdad $\eta_h = \eta_k$ que le sirve de base.

129.—*Forma de las funciones enteras de las raices de la ecuacion del círculo.*

—

Toda funcion de las raices de la ecuacion del círculo que permanezca invariable, cuando en ella se sustituya r por r^{g^e}, puede ser representada por una funcion lineal de los períodos η, cuyos coeficientes serán funciones enteras de los contenidos en la funcion dada, siempre que estos coeficientes dados sean enteros, ó funciones enteras de la raiz α.

Supongamos que la funcion propuesta de las raices de la ecuacion del círculo se haya reducido á su forma normal, en cuyo caso tendrá por expresion la siguiente ya conocida:

$$f(r) = a_0 r + a_1 r^g + a_2 r^{g^2} + \ldots\ldots + a_{p-2} r^{g^{p-2}}.$$

Segun la hipótesis del teorema enunciado, las funciones $f(r)$ y $f(r^{g^e})$ serán iguales, y lo serán tambien por consecuencia:

$$f(r^{g^{2e}}) = f(r^{g^{3e}}) = \ldots\ldots = f(r^{g^{(f-1)e}})$$

y, como todas estas f funciones son valores equivalentes de la normal, ésta será por lo tanto:

$$f(r) = \frac{1}{f}\left[f(r) + f(r^{g^e}) + \ldots\ldots + f(r^{g^{(f-1)e}})\right].$$

Para efectuar la suma de las funciones inclusas en el paréntesis, del

término general $a_k . r^{g^k}$, de la forma normal $f(r)$, se deducen las expresiones $\frac{1}{f} a_k . \eta_k$, y se halla la siguiente:

$$f(r) = \frac{1}{f}\left(a_0 \eta_0 + a_1 \eta_1 + \ldots\ldots + a_{p-2} . \eta_{p-2}\right)$$

ó bien, reuniendo los períodos iguales (*):

$$f(r) = m_0 \eta_0 + m_1 \eta_1 + \ldots\ldots + m_{e-1} \eta_{e-1} .$$

Del procedimiento empleado para deducir esta última expresion resulta que sus coeficientes m son funciones enteras, con coeficientes racionales, de los coeficientes a que figuran en la funcion propuesta; y, como estos son enteros, tambien lo serán los coeficientes m; porque las dos expresiones que comprenden los unos y los otros respectivamente, como de la misma forma normal $f(r)$, tienen que ser, segun lo que antes demostramos, idénticas.

De esta proposicion se desprenden corolarios interesantes:

1.° *Toda funcion entera de los períodos* η_1, *puede ser expresada por*

(*) Téngase en cuenta para comprender esto mejor, que si las expresiones de la forma normal, resultantes de sustituir en ella por $r^{g^e}, r^{g^{2e}}, \ldots\ldots r^{g^{(f-1)e}}$ la raiz r, son equivalentes, se verificarán tambien las igualdades:

$$a_0 = a_e = a_{2e} = \ldots\ldots = a_{(f-1)e}$$

$$a_1 = a_{e+1} = a_{2e+1} = \ldots\ldots = a_{(f-1)e+1}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$a_{e-1} = a_{2e-1} = a_{3e-1} = \ldots\ldots = a_{fe-1}$$

una funcion lineal de los mismos, cuyos coeficientes serán enteros ó racionales, conforme lo que sean los de la funcion propuesta. Porque tales períodos permanecen invariables cuando en ellos se sustituye r por r^{g^e}.

Como caso particular de estas funciones enteras desarrollaremos en este lugar el producto de dos períodos, no sólo para patentizar la verdad del corolario, ya, en general, demostrada, sino más bien por sus aplicaciones ulteriores.

El producto de los dos períodos

$$\eta_0 = \sum_{s=0}^{s=f-1} r^{g^{es}} \quad \text{y} \quad \eta_k = \sum_{t=0}^{t=f-1} r^{g^{et+k}}$$

puede escribirse así:

$$\eta_0 \cdot \eta_k = \sum_{s=0}^{s=f-1} \sum_{t=0}^{t=f-1} r^{g^{es}(1+g^{et+k})}$$

en el supuesto de que, para un valor determinado y constante de s, las expresiones $t+s$ y t representen simultáneamente valores congruentes (mod. f) con los números $0, 1, 2, \ldots\ldots f-1$.

Al efectuar desde luego la suma respecto de la variable s, debemos distinguir dos casos: 1.° que el factor binomio que figura en el exponente de r, para cierto valor de t, verifique la congruencia

$$1 + g^{et+k} \equiv 0 \,(\text{mod. } p); \qquad (1)$$

ó 2.°, que dicho binomio satisfaga á esta otra:

$$1 + g^{et+k} \equiv g^{ez+k} \,(\text{mod. } p) \qquad (2)$$

en la cual puede recibir h cualquiera de los valores $0, 1, 2, \ldots\ldots e-1$, y z á su vez uno de los siguientes: $0, 1, 2, \ldots\ldots f-1$.

En el primero, como los exponentes de r son siempre *cero*, la parte correspondiente de la doble suma se reduce á la de f unidades, ó á f; y en el segundo, dicha parte se convierte en el período:

$$\sum_{s=0}^{s=f-1} r^{g^{e(s+z)+h}} = \eta_h .$$

Mas la congruencia (1), por ser g raiz primitiva y, de consiguiente, *no-resto* de p, equivale á la ecuacion

$$et + k = \tfrac{1}{2}(p-1) = \tfrac{1}{2}ef .$$

Esta ecuacion, si f es par, exige que sea k divisible por e, y para esto, como k es un resto de e, que sea $k=0$; y, por consecuencia, $t = \frac{1}{2}f$, único valor de t que entónces la satisface; y, si f es impar, que k sea divisible por $\frac{1}{2}e$, sin ser *cero;* pues, si lo fuera, resultaria $et = \frac{1}{2}ef \equiv 0 \pmod{e}$, para lo cual deberia ser f par, contra lo supuesto; y, como entre los valores que puede recibir k, sin ser cero, solo hay uno, divisible por $\frac{1}{2}e$, que es este mismo, será finalmente $k = \frac{1}{2}e$ y, por consecuencia, $t = \frac{1}{2}(f-1)$.

Luego, si convenimos en que el símbolo $n^{(k)}$ represente la *unidad*, siempre que f sea par y $k=0$, ó que f sea impar y $k = \frac{1}{2}e$, esto es, siempre que se realice el primero de los casos en un principio distinguidos, definido por la congruencia (1), ó su ecuacion equivalente; y

el *cero*, cuando esto no se verifique; y designamos por este otro símbolo, m_h^k, el número de valores de t para los cuales ocurrirá el segundo caso, de tal modo que sea $m_h^k = 0$, cuando al sistema de valores h, k no corresponda otro sistema t, z, que satisfaga á la congruencia (2), el producto de los dos períodos η_0 y η_k, puede ser expresado bajo esta forma más explícita:

$$\eta_0 . \eta_k = n^{k'} . f + m_0^k . \eta_0 + m_1^k . \eta_1 + \ldots\ldots + m_{e-1}^k . \eta_1^{e-1} \qquad (3)$$

Si en esta ecuacion ponemos r^{g^m} en vez de r, con lo cual los períodos $\eta_0, \eta_1 \ldots\ldots \eta_{e-1}$ se habrán permutado circularmente, corriéndose m lugares, se obtiene la siguiente:

$$\eta_m . \eta_{m+k} = n^{k'} . f + m_0^k . \eta_m + m_1^k . \eta_{m+1} + \ldots\ldots + m_{e-1}^k . \eta_{m-1} \qquad (4)$$

En estas dos últimas expresiones se ve claramente que el producto de los dos períodos elegidos es, en efecto, una funcion lineal de todos los períodos f-membres; y, si los dos períodos fuesen iguales, el producto se transformaria en *potencia* (funcion entera tambien) con la misma propiedad.

2.° Estos períodos f-membres, en el supuesto de ser $e = 1$ y, por consecuencia, $f = p - 1$, se reducen á uno solo, á saber:

$$\eta_0 = [1] + [g] + [g^2] + \ldots\ldots + [g^{p-2}]$$

cuyo valor, que es la suma de todas las raices de la ecuacion del círcu-

lo, es igual á -1. Toda funcion entera, con coeficientes enteros, de este período, ó bien de las raices de la ecuacion del círculo, puede representarse por una funcion lineal del mismo período; y, como esta funcion lineal es un número entero, tambien lo será la funcion entera equivalente: luego

Toda funcion entera, con coeficientes enteros, de las raices de la ecuacion del círculo, que no se altere áun cuando en ella se sustituya r *por* r^g, *tiene un valor tambien entero.*

3.° Los períodos realizan precisamente esta condicion de permanecer invariables aun cuando en ellos se cambie la r en r^g; y lo mismo acontece, por consecuencia, en cualquiera funcion simétrica de los mismos, de donde se concluye que:

Toda funcion simétrica, entera y con coeficientes enteros, de los períodos es asimismo equivalente á un número entero.

130.—*De la ecuacion irreducible cuyas raices son los períodos f-membres.*

Los e *períodos f-membres son raices de una ecuacion irreducible de grado* e, *con coeficientes enteros, y del género de las abelianas, como la ecuacion del círculo.* La ecuacion cuyas raices son los períodos f-membres es ésta:

$$F(x) = (x - \eta_0)\,(x - \eta_1) \cdots (x - \eta_{e-1}) = 0 \qquad (a)$$

cuyos coeficientes, como funciones simétricas enteras de los e períodos, son, segun acabamos de decir, números enteros.

Para demostrar que esta ecuacion es irreducible, supongamos que no lo sea, y que su primer miembro, de consiguiente, contenga un factor racional $\varphi(x)$. Este factor comprenderá necesariamente alguno de los períodos ó raices de la ecuacion (a): y, si designamos por η_h tal período, la ecuacion $\varphi(\eta_h) = 0$ será racional, tendrá la raiz r,

comun con la ecuacion del círculo, y será satisfecha, en consecuencia, por las otras raices r^g, r^{g^2} ..... $r^{g^{e-1}}$ de esta última (125). Efectuando esta sustitucion de r por las raices indicadas en la ecuacion $\varphi(\eta_h) = 0$, se obtienen las siguientes:

$$\varphi(\eta_{h+1}) = 0, \quad \varphi(\eta_{h+2}) = 0, \ldots\ldots \varphi(\eta_{h+e-1}) = \varphi(\eta_{h-1}) = 0.$$

Y este resultado manifiesta el absurdo de que la ecuacion racional $\varphi(x) = 0$, cuyo grado es inferior á e, contenga, sin embargo, las e raices $\eta_0, \eta_1 \ldots\ldots \eta_{e-1}$.

Para demostrar ahora que la ecuacion (a) es tambien abeliana, ó, lo que es igual, que sus raices pueden deducirse, como las de la ecuacion del círculo, mediante la misma operacion racional, de cualquiera de ellas, recordaremos (129—1.°) que toda potencia (funcion entera) de un período η_h, es una funcion lineal de todos los períodos, y, por consecuencia, serán ciertas las igualdades:

$$\eta_h = m'_0 \eta_0 + m'_1 \eta_1 + \ldots\ldots + m'_{e-1} \eta_{e-1}$$

$$\eta_h^2 = m''_0 \eta_0 + m''_1 \eta_1 + \ldots\ldots + m''_{e-1} \eta_{e-1}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\eta_h^{e-1} = m_0^{(e-1)} \eta_0 + m_1^{(e-1)} \eta_1 + \ldots\ldots + m_{e-1}^{(e-1)} \eta_{e-1}$$

á las cuales podemos agregar esta otra ya conocida:

$$-1 = \eta_0 + \eta_1 + \ldots\ldots + \eta_{e-1}.$$

Despejando un período cualquiera η_k de estas e ecuaciones, se obtiene otra de la forma siguiente:

$$D.\,\eta_k = A_0 + A_1\eta_k + A_2\eta_k^2 + \ldots + A_{e-1}\eta_k^{e-1}:$$

cuyos coeficientes son enteros que no se anulan en totalidad, y de la cual puede deducirse el valor del período η_k en funcion del η_k, dividiendo por el coeficiente D, en atencion á que este D no puede ser cero; porque, de serlo, resultaria la ecuacion:

$$0 = A_0 + A_1\eta_k + A_2\eta_k^2 + \ldots + A_{e-1}\eta_k^{e-1},$$

no idéntica, y de grado $e-1$, que tendria la raiz η_k comun con la irreducible $F(x)=0$, de grado e: lo cual es imposible (125).

Conclúyese de lo dicho la exactitud de la ecuacion

$$\eta_1 = \Theta(\eta_0),$$

siendo Θ el símbolo de una funcion entera: ecuacion que puede desde luego considerarse como racional, y satisfecha por la raiz r; y como invariable tambien, áun cuando en ella se sustituya r por r^g, r^{g^2} ..... etc.; pero de tal sustitucion se desprenden estas otras ecuaciones:

$$\eta_2 = \Theta(\eta_1),\ \eta_3 = \Theta(\eta_2),\ \ldots\ldots \eta_{e-1} = \Theta(\eta_{e-2}),\ \eta_0 = \Theta(\eta_{e-1})$$

que prueban finalmente lo que pretendíamos demostrar.

Resuelta la ecuacion (a), es claro que cada una de sus raices representará el valor de uno de los e períodos η; pero la raiz r de la ecuacion del círculo, de cuya eleccion sabemos (128—2.ª) depende el valor de éstos, permanece todavía arbitraria, y no es posible así decidir cuál de los períodos será el que exprese una raiz α de la primera. Supongamos ahora que, para esta raiz determinada α, de la ecuacion (a) y

otra elegida r, de la del círculo, se verifique la igualdad $\eta_h = \alpha$. Entónces sólo tendremos que variar la significacion de r, haciendo que exprese uno de los términos del período η_h, para que cambie asimismo la significacion de los símbolos $\eta_0, \eta_1 \ldots\ldots \eta_{e-1}$, convirtiéndose en η_0 el que antes era η_h. De donde se infiere que, eligiendo un valor conveniente de r, siempre podremos establecer la igualdad $\eta_0 = \alpha$: con lo cual se concreta la indeterminacion de la raiz r á ser uno de los términos del período η_0, ya en otro lugar (128) completamente determinados.

Conocido de este modo el período η_0, todos los demas, como acabamos de ver, se hallan expresados por funciones racionales del mismo, y esto quiere decir que, para hallar sus valores, solamente tendremos que resolver ecuaciones lineales.

131.—*De la ecuacion irreducible cuyas raices son los términos de un período.*

—

Los f términos de un período η_h son raices de una ecuacion $F_h(x) = 0$, de grado f, cuyos coeficientes son funciones lineales y enteras de los e períodos η, y cuyo primer miembro no puede ser descompuesto en factores de iguales propiedades que los coeficientes. Los coeficientes de la ecuacion que tiene por raices los términos,

$$[g^h],\ [g^{h+e}],\ [g^{h+2e}],\ \ldots\ldots [g^{h+(f-1)e}], \qquad (h)$$

del período η_h, son funciones simétricas de estos f términos, é invariables, por consecuencia, ante cualquiera permutacion de los mismos; y, como entre tales permutaciones se halla comprendida la circular que en dichos términos ó raices produce el cambio de la r por la r^{g^e}, re-

sulta (129), en efecto, que los coeficientes mencionados son funciones lineales y enteras de los períodos η.

Para demostrar ahora que la ecuacion $F_h(x) = 0$ es irreducible en el sentido que dice el teorema, admitamos, en contrario, que su primer miembro contenga un factor $\varphi(x, \eta_0, \eta_1 \ldots\ldots \eta_{e-1})$ cuyos coeficientes sean tambien funciones lineales y enteras de los períodos η, y el cual debe contener alguna de las raices de la ecuacion $F_h(x) = 0$, ó convertirse en cero para uno, por lo menos, de los términos (h). Si reemplazamos los símbolos η por sus expresiones correspondientes, obtendremos una ecuacion en r, con coeficientes racionales, que será satisfecha por todas las raices de la ecuacion del círculo, y, de consiguiente, como incluidos en ellas, por los términos del período η_h, distintos del que antes, ó de los que antes supusimos convertian en cero el factor designado. De lo cual resulta, teniendo en cuenta tambien que los períodos permanecen invariables, aunque se cambie por otra, cualquiera de las raices mencionadas, que la ecuacion

$$\varphi(x, \eta_0, \eta_1 \ldots\ldots \eta_{e-1}) = 0,$$

de grado menor que f necesariamente, es satisfecha cuando menos por las f raices comprendidas en el período η_h: y esto es absurdo.

Aplicando la ecuacion $F_h(x) = 0$ á todos los períodos se obtienen las siguientes:

$$F_0(x) = 0, F_1(x) = 0, \ldots\ldots F_{e-1}(x) = 0 \qquad (b)$$

de cuya resolucion depende la resolucion completa de la ecuacion del círculo; pero no es preciso resolverlas todas; basta conocer las soluciones de una sola; porque ya sabemos que, conocida una raiz de la ecuacion del círculo, todas las demás se deducen de ella por elevacion á potencias. Ahora bien, para poder formar las ecuaciones (b) es necesario y suficiente haber antes resuelto la ecuacion (a), ó haber determinado los e períodos f-membres; y una vez hecho esto, vemos que la resolucion de la ecuacion del círculo, de grado $p - 1 = ef$, se convier-

te en la mas sencilla de la ecuacion (a), de grado e, y una de las ecuaciones (b) de grado f; ó bien que, resuelta la ecuacion (a), puede descomponerse la funcion X en e factores de grado f que son á la manera de X irreducibles.

Prosigamos esta descomposicion y supongamos para ello $f = e'.f'$: entónces será $p - 1 = e e' f'$; y las raices de la ecuacion del círculo podremos distribuirlas en los $e e'$ períodos f'-membres, siguientes:

$$\eta'_0 = [g^0] + [g^{ee'}] + [g^{2ee'}] + \ldots\ldots + [g^{(f'-1)ee'}]$$

$$\eta'_1 = [g^1] + [g^{ee'+1}] + [g^{2ee'+1}] + \ldots\ldots + [g^{(f'-1)ee'+1}]$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\eta'_e = [g^e] + [g^{ee'+e}] + [g^{2ee'+e}] + \ldots\ldots + [g^{(f'-1)ee'+e}]$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\eta'_{2e} = [g^{2e}] + [g^{ee'+2e}] + [g^{2ee'+2e}] + \ldots\ldots + [g^{(f'-1)ee'+2e}]$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\eta'_{ee'-1} = [g^{ee'-1}] + [g^{2ee'-1}] + [g^{3ee'-1}] + \ldots\ldots + [g^{f'ee'-1}]$$

Cada grupo de e' períodos de los precedentes constituye uno de los f-membres antes definidos, como por ejemplo:

$$\eta_0 = \eta'_0 + \eta'_e + \eta'_{2e} + \ldots\ldots + \eta'_{(e'-1)e}.$$

Tanto estos como los anteriores están sujetos á las mismas leyes, si bien con las consiguientes modificaciones. Sólo recordaremos especial-

mente aquí la de que cada uno de los períodos f'-membres es una funcion racional y entera de cualquiera de los otros del mismo género.

132.—*De la ecuacion cuyas raices son los e' períodos que componen un f-membre.*

Los e' períodos, tales como

$$\eta'_0,\ \eta'_e,\ \eta'_{2e} \ldots\ldots \eta'_{(e'-1)e}$$

que componen un f-membre η_0, *son raices de una ecuacion irreducible de grado e', cuyos coeficientes son funciones lineales de estos períodos f-membres.*

En efecto, los coeficientes de la ecuacion

$$F_0'(x) = \left(x-\eta'_0\right)\left(x-\eta'_e\right)\left(x-\eta'_{2e}\right) \ldots\ldots - \left(x-\eta'_{(e'-1)e}\right) = 0$$

que tiene por raices los e' períodos dichos, son, como repetidas veces hemos recordado, funciones simétricas de estos períodos, las cuales no se alteran por la sustitucion de r por r^{g^e}, y pueden ser expresadas, en consecuencia (129), mediante los períodos f-membres primitivos.

El ser la ecuacion $F_0'(x) = 0$ irreducible, se deduce de que lo es la anteriormente considerada $F_0(x) = 0$. Designemos, pues, por $\varphi'\left(x, \eta_0 \eta_1 \ldots\ldots \eta_{e-1}\right)$ un factor (cuyos coeficientes sean tambien funciones lineales de los períodos f-membres) de la funcion $F_0'(x)$. Este factor debe contener alguna de las raices de la ecuacion $F_0'(x) = 0$, y reducirse á cero, por lo tanto, para el valor $x = \eta'_{he}$, por ejemplo. La ecuacion así resultante,

$$\varphi'\left(\eta'_{he},\ \eta_0,\ \eta_1 \ldots\ldots \eta_{e-1}\right) = 0,$$

admitiendo que sea satisfecha por una raiz r de la ecuacion $F_0(x) = 0$, debe subsistir áun cuando se sustituya r por las otras raices $r^{g^e}, r^{g^{2e}} \ldots\ldots r^{g^{(e'-1)e}}$. A pesar de esta sustitucion, los períodos $\eta_0, \eta_1 \ldots\ldots \eta_{e-1}$ permanecen inalterables; pero el η'_{he} se convierte, á causa de la misma, sucesivamente en los períodos $\eta'_{(h+1)e}, \ldots\ldots \eta'_{(h-1)e}$: de lo cual resulta que la ecuacion $\varphi' = 0$, de grado menor que e', comprende más raices que unidades tiene su grado: y esto es imposible.

Determinados por la ecuacion (a) los períodos f-membres, podemos establecer las e ecuaciones, de grado e', que á continuacion figuran:

$$F'_0(x) = 0,\ F'_1(x) = 0,\ F'_2(x) = 0, \ldots\ldots F'_{e-1}(x) = 0; \qquad (c)$$

cuyas raices son respectivamente cada uno de los e' períodos de f' términos, ó f'-membres, y las cuales nos sirven para determinar estos períodos f'-membres en funcion de los f-membres. Pero no hay precision de resolver todas las ecuaciones (c): basta resolver una de ellas; porque, conocido uno de los períodos f'-membres, los restantes son, como sabemos, funciones racionales del mismo.

Hallados, mediante la resolución de una de las ecuaciones (c), de grado e', los períodos f'-membres, cada uno de los e factores, de grado f, en los cuales ya se descompuso X, se convierte en reducible; y la funcion X puede así descomponerse, conforme antes dijimos, en ee' factores de grado f', los cuales son tambien, al modo que los otros, irreducibles.

Prolongando estas descomposiciones llegaremos, por último, á resolver la funcion X en factores de primer grado, y entónces las raices de la ecuacion del círculo $X = 0$, nos serán inmediatamente conocidas. En la posibilidad de estas descomposiciones sucesivas se funda, como en un principio indicamos, el método de Gauss para resolver la ecuacion del círculo.

Todo el procedimiento hasta aquí explicado se resume en la regla que sigue:

«Elíjase ante todo una raiz primitiva g del módulo ó grado p, y calcúlense los restos mínimos (mod. p) de las potencias de g, desde la

0 hasta la $p-2$. Descompóngase $p-1$ en sus factores $a, b, c, d, \ldots k$, y establézcanse las igualdades:

$$\frac{p-1}{a} = bcd.....k = A; \frac{p-1}{ab} = cd.....k = B; \frac{p-1}{abc} = d.....k = C, \text{ etc.}$$

Distribúyanse todas las raices de la ecuacion $X=0$ en a períodos η_1, de A términos cada uno; y como estos períodos son raices de una ecuacion con coeficientes enteros, resolviéndola, hallaremos los a períodos η_1, y habremos descompuesto el polinomio X en a factores, de grado A, cuyos coeficientes nos serán tambien conocidos por resultado de la misma operacion.

Distribúyanse luego las raices de cada uno de los períodos η_1, en b períodos menores η_1', de B términos; y, como los períodos η_1', componentes de uno de los η_1, son raices de una ecuacion, de grado b, cuyos coeficientes son funciones lineales de estos períodos η_1, resolviéndola, hallaremos los ab períodos η_1', y habremos descompuesto á X en ab factores, del grado B, perfectamente definidos.

Distribúyanse del propio modo las raices ó términos de cada uno de los períodos η_1', en c períodos menores η_1'', de C términos; y como los períodos η_1'', componentes de uno de los η_1', son raices de una ecuacion, de grado c, cuyos coeficientes son funciones lineales de estos períodos η_1', resolviéndola, determinaremos todos los abc períodos η_1'', y lograremos descomponer á X en abc factores, de grado C, sin ambigüedad ó indecision de ningun género.

Y repitiendo la misma série de operaciones cuantas veces fuese menester, llegaremos, por último, á determinar los períodos de un sólo término, ó las raices propiamente dichas de la ecuacion $X=0$. Cada número k, de estas raices, constituirá uno de los períodos inmediatamente anteriores, dependientes á su vez de otra ecuacion del grado k, cuyos coeficientes son funciones lineales de los períodos que tambien inmediatamente le preceden. Y resolviendo la nueva ecuacion, y procediendo luégo, como queda explicado, obtendremos por fin las mismas raices de la ecuacion del círculo buscadas.

133.—*Casos en que puede dividirse la circunferencia con la regla y el compás.—Distribucion conveniente de* $p-1$ *en sus factores.*

En cuanto precede no hemos determinado la descomposicion en factores de $p-1$, sino que tal descomposicion la hemos dejado arbitraria. Sin embargo, como lo conveniente en general es que las ecuaciones auxiliares para resolver la del círculo sean del menor grado posible, es preciso descomponer $p-1$ en sus factores simples, ya sean iguales ó desiguales.

Al efectuar así esta descomposicion, puede ocurrir que todos los factores primos, contenidos en $p-1$; sean iguales á 2: en cuyo supuesto tendrá p la forma 2^m+1; las ecuaciones auxiliares correspondientes serán todas de segundo grado; y sus raices, por consecuencia, se expresarán por radicales tambien cuadrados. Ahora bien, como todas las expresiones que no contengan otras cantidades irracionales sino las de segundo grado, pueden ser construidas geométricamente con la regla y el compás, resulta que:

Cuando p *sea un número primo, de la forma* 2^m+1, *la division de la circunferencia en* p *partes iguales, é inscripcion en ella del polígono del mismo número de lados puede efectuarse con la regla y el compás.*

En este caso se hallan el triángulo y el pentágono regulares, como ya sabemos; y los polígonos de 17, 257, etc., lados. Pero, no representando la forma 2^m+1 un número primo para cualquier valor de m, seria conveniente saber, en general, cuáles habrian de ser los valores de este exponente que convirtieran aquella forma en un número primo. Acerca de esta cuestion interesante sólo podemos decir que desde luego el exponente m debe ser potencia del número 2; porque, si fuera divisible por un número impar, estableciendo la igualdad consiguiente $m=m'(2n+1)$, de la fórmula conocida

$$x^{2n+1}+1=(x+1)\left(x^{2n}-x^{2n-1}+x^{2n-2}-\ldots\ldots+x^2-x+1\right),$$

resultaria que $2^{m'(2n+1)}+1$ era divisible por $2^{m'}+1$; y, por consecuencia, compuesto el número $2^{m}+1$. Mas tampoco son primos todos los números de la forma $2^{2^{n}}+1$; pues para el valor de $n=5$, se obtiene el número

$$2^{2^{5}}+1=4294967297,$$

divisible por 641. De todo lo cual se desprende, en conclusion, que aún no podemos decidir si existen, ó no, infinitos casos en que pueda ser dividida la circunferencia, mediante la regla y el compás solamente.

Tambien debemos notar la conveniencia de elegir para último factor el número primo 2, en la descomposicion del siempre par, $p-1$. De este modo, cada uno de los períodos contendrá un número par de términos, y será una suma de los últimos períodos bimembres,

$$[1]+[g^{\frac{p-1}{2}}]\,.\,[g]+[g^{\frac{p-1}{2}+1}]\,.\,[g^{2}]+[g^{\frac{p-1}{2}+2}]\,.\,.\,.\,.$$

$$.\,.\,.\,.\,[g^{\frac{p-3}{2}}]+[g^{\frac{p-3}{2}}\,.\,g^{\frac{p-1}{2}}]:$$

los cuales, recordando (106) que g es *no-resto* de p, y, por consecuencia, $g^{\frac{p-1}{2}}\equiv -1 \pmod{p}$, se podrán escribir del modo siguiente:

$$[1]+[-1],\ [g]+[-g],\ [g^{2}]+[-g^{2}],\,.\,.\,.\,.$$

$$.\,.\,.\,.\,[g^{\frac{p-3}{2}}]+[-g^{\frac{p-3}{2}}].$$

Todos estos períodos tienen valores reales; pues haciendo

$$r=cos.\frac{2k\pi}{p}+i\,sen.\frac{2k\pi}{p},$$

serán:

$$r^{g^h} = cos.\frac{2kg^h.\pi}{p} + i\,sen.\frac{2kg^h.\pi}{p}$$

$$r^{-g^h} = cos.\frac{2kg^h.\pi}{p} - i\,sen.\frac{2kg^h.\pi}{p}$$

y, por consiguiente:

$$r^{g^h} + r^{-g^h} = 2\,cos.\frac{2kg^h.\pi}{p}: \text{ cantidad real.}$$

Manifiesta es la ventaja de que tengan valores reales las raices de las ecuaciones auxiliares; pero resalta más todavía cuando se pasa á las raices imaginarias de la ecuacion del círculo desde los períodos bimembres, ó raices de las últimas ecuaciones de segundo grado.

Ejemplos.

1.° *Dividir la circunferencia en cinco partes iguales, ó inscribir en ella el pentágono regular.* Eligiendo, en conformidad con la regla prescrita, la raiz primitiva $g = 2$ del número $p = 5$, tendremos:

$2^0, 2^1, 2^2, 2^3$	*potencias.*
$0\ ,\ 1\ ,\ 2\ ,\ 3$	*índices.*
$1\ ,\ 2\ ,\ 4\ ,\ 3$	*números correspondientes.*

Descomponiendo ahora el número $p - 1 = 4$, en sus dos factores $2 \cdot 2 = e \cdot f$, las raices r, r^2, r^3, r^4, de la ecuacion propia de este caso,

$$\frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1 = 0,$$

se distribuirán en los dos períodos bimembres:

$$\eta_0 = r + r^4, \qquad \eta_1 = r^2 + r^3:$$

los cuales son raices de la ecuacion de segundo grado:

$$x^2 - (\eta_0 + \eta_1)x + \eta_0 \eta_1 = 0.$$

Y esta ecuacion, teniendo presente que

$$\eta_0 + \eta_1 = r + r^2 + r^3 + r^4 = -1,$$

$$\eta_0 \eta_1 = r^3 + r^2 + r + r^4 = -1,$$

se convierte en esta otra:

$$x^2 + x - 1 = 0$$

cuyas dos raices son:

$$\frac{-1+\sqrt{5}}{2} \quad \text{y} \quad \frac{-1-\sqrt{5}}{2};$$

representando cualquiera de ellas el valor del período η_0, y la otra el del η_1. Si establecemos, pues, las igualdades

$$\eta_0 = \frac{-1+\sqrt{5}}{2}, \qquad \eta_1 = \frac{-1+\sqrt{5}}{2},$$

deberemos elegir la raiz r entre las dos del período η_0, ya arbitrariamente determinado.

La ecuacion de segundo grado que tiene por raices las dos que constituyen este período η_0, es la siguiente:

$$x^2 - (r + r^4)x + r \cdot r^4 = x^2 - \eta_0 x + 1 = 0.$$

Resolviéndola, podemos establecer la igualdad

$$r = \frac{\eta_0}{2} + \sqrt{\frac{\eta_0^2}{4} - 1}$$

que se transforma, poniendo por η_0 el valor que le asignamos, en esta otra:

$$r = \frac{-1 + \sqrt{5} + \sqrt{(-1)\,(2\sqrt{5} + 10)}}{4} =$$

$$= \frac{-1 + \sqrt{5} + i\sqrt{10 + 2\sqrt{5}}}{4}.$$

De los dos períodos, η_0 y η_1, el primero es evidentemente positivo, y negativo el otro. Los valores de estos dos períodos, haciendo como siempre, y en particular para este caso,

$$r = cos.\frac{2k\pi}{5} + i\,sen.\frac{2k\pi}{5},$$

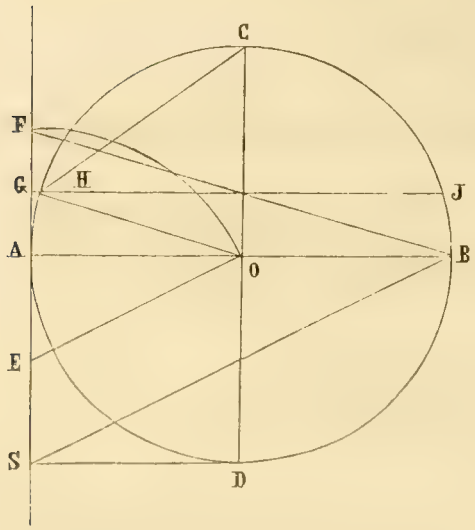
son:

$$\eta_0 = r + r^{-1} = 2\,cos.\frac{2k\pi}{5}; \quad \eta_1 = r^2 + r^{-2} = 2\,cos.\frac{4k\pi}{5}.$$

Luego habremos de elegir entre $k = 1$ ó $k = 4$ para justificar el valor que atribuimos á η_0; resultando en el primer supuesto:

$$r = cos.\frac{2\pi}{5} + i\,sen.\frac{2\pi}{5}; \text{ y, por tanto: } \eta_0 = 2\,cos.\frac{2\pi}{5}.$$

Construccion.—Como el número 5 es de la forma 2^m+1, este problema puede ser resuelto mediante una construccion geométrica con el auxilio únicamente de la regla y el compás. En efecto: en la circunferencia que se trata de dividir en cinco partes, y cuyo radio suponemos igual á la unidad, trácense los dos diámetros perpendiculares entre sí, AB y CD, y por sus extremos respectivos A y D, dos tangentes que se cortarán en el punto S. Divídase, como indica la figura, la distancia AS en dos partes iguales, y uniendo su punto medio E, con el centro O, tendremos:



$$OE=\sqrt{OA^2+AE^2}=\sqrt{1+\frac{1}{4}}=\frac{1}{2}\sqrt{5}\,.$$

Haciendo centro ahora en E, descríbase con el radio EO un arco que cortará en F á la tangente prolongada AS, y será:

$$AF=EF-AE=OE-AE=\frac{1}{2}\sqrt{5}-\frac{1}{2}=$$

$$=\frac{-1+\sqrt{5}}{2}=r_{10}=2\,cos.\,\frac{2\pi}{5}.$$

Y, dividiendo por mitad el trozo AF, como la figura manifiesta,

la paralela GHJ al diámetro AB, trazada por el punto medio G, de dicha distancia AF, cortará á la circunferencia en dos puntos H y J, que son dos vértices del pentágono, siendo el lado de éste cualquiera de las distancias CH ó CJ; puesto que

$$\frac{1}{2}AF = AG = cos.\ \frac{2\pi}{5} = cos.\ 72^0.$$

2.°—*Dividir la circunferencia en trece partes iguales.* Eligiendo la raiz primitiva $g = 6$, del número $p = 13$, los índices (base 13) y los números correspondientes serán:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	*índices.*
1, 6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11	*números.*

Descomponiendo ahora el número $p - 1 = 12 = 3 . 2 . 2$, las raices de la ecuacion

$$\frac{x^{13} - 1}{x - 1} = 0,$$

se distribuirán en los *tres* períodos *quatri*-membres:

$$\eta_0 = r + r^8 + r^{12} + r^5,\ \eta_1 = r^6 + r^9 + r^7 + r^4,$$

$$\eta_2 = r^{10} + r^2 + r^3 + r^{11}$$

los cuales serán raices de la ecuacion de tercer grado:

$$x^3 - (\eta_0 + \eta_1 + \eta_2)x^2 + (\eta_0\eta_1 + \eta_1\eta_2 + \eta_0\eta_2)\,x - \eta_0\eta_1\eta_2 = 0.$$

Lo primero que debemos hacer ahora es determinar los valores nu-

méricos de los coeficientes de esta ecuacion. En cuanto al segundo ya sabemos que

$$\eta_0 + \eta_1 + \eta_2 = -1.$$

Para determinar los productos binarios que forman el tercero, aplicaremos la expresion (129—1.°). Segun ella, tendremos:

$$\eta_0 \eta_k = \eta_0 \eta_1 = n^{(1)} . f + m_0^1 . \eta_0 + m_1^1 . \eta_1 + m_2^1 . \eta_2 .$$

El símbolo $n^{(1)}$ es cero por ser $k = 1$. Para hallar el valor del símbolo m_0^1, en la congruencia

$$1 + 6^{3t+1} \equiv 6^{3z} \text{ (mod. 13)},$$

que se deduce de la general (2), haciendo en ella $e=3$, $k=1$, $h=0$, $p=13$, pondremos en lugar de z sucesivamente los valores 0, 1, 2, 3; con lo cual se obtienen respectivamente los de las potencias:

$$6^0 \equiv 1;\ 6^3 \equiv 8;\ 6^6 \equiv 12;\ 6^9 \equiv 5 \text{ (mod. 13)}:$$

y ya no es difícil encontrar cuántos podrá recibir t que satisfagan á la congruencia anterior para cada uno de los restos 1, 8, 12, 5. Ahora bien, de las cuatro congruencias correspondientes á estos restos,

$$1 + 6^{3t+1} \equiv 1,\ \equiv 8,\ \equiv 12,\ \equiv 5 \text{ (mod. 13)},$$

solamente dos, la segunda y la cuarta, son satisfechas por los valores de t respectivamente $t = 2$, $t = 3$, y nada más que por estos *dos* valores: luego m_0^1 será igual á 2. Mediante el mismo procedimiento se encuentran para los símbolos m_1^1 y m_2^1 sus valores respectivos que son

en este caso: $m_1^1 = 1$, $m_2^1 = 1$; y así, el producto de los dos períodos en cuestion resulta:

$$\eta_0 \eta_1 = 2\eta_0 + \eta_1 + \eta_2$$

y tambien, por el mismo método, se hallan:

$$\eta_1 \eta_2 = \eta_0 + 2\eta_1 + \eta_2$$

$$\eta_0 \eta_2 = \eta_0 + \eta_1 + 2\eta_2$$

$$\eta_0 \eta_0 = 4 + 2\eta_1 + \eta_2$$

De estas igualdades, sumando las tres primeras, se deduce:

$$\eta_0 \eta_1 + \eta_1 \eta_2 + \eta_0 \eta_2 = 4\left(\eta_0 + \eta_1 + \eta_2\right) = -4;$$

y, multiplicando la segunda por η_0, despues de las sustituciones y reducciones consiguientes, se encuentra:

$$\eta_0 \eta_1 \eta_2 = 4 + 5\left(\eta_0 + \eta_1 + \eta_2\right) = 4 - 5 = -1.$$

La ecuacion de tercer grado, cuyas raices son los tres períodos *quatri*-membres, η_0, η_1, η_2, se reduce, por consecuencia, á la siguiente:

$$x^3 + x^2 - 4x + 1 = 0.$$

Resuelta esta ecuacion, los tres períodos mencionados pueden considerarse conocidos. Descompongamos ahora cada uno de ellos en dos, y por lo tanto, los tres, en seis períodos η' de dos términos, ó bimembres, de modo que sea:

$$\eta_0 = \eta'_0 + \eta'_3, \qquad \text{y} \qquad \eta'_0 = r + r^{12}, \; \eta'_3 = r^8 + r^5.$$

Estos dos períodos nuevos, η', serán raices de la ecuacion

$$x^2 - \left(\eta'_0 + \eta'_3\right) x + \eta'_0 \eta'_3 = 0,$$

ó bien, como $\eta'_0 \eta'_3 = \eta_1$, de esta otra equivalente:

$$x^2 - \eta_0 x + \eta_1 = 0,$$

mediante la cual se hallarán los períodos η'_0 y η'_3. Hallados éstos, se formará la ecuacion, cuyas raices sean las dos de que consta el η'_0, á saber:

$$x^2 - \left(r + r^{12}\right) x + r \cdot r^{12} = 0,$$

que tambien puede escribirse como sigue:

$$x^2 - \eta'_0 x + 1 = 0.$$

Y resolviendo esta ecuacion, vendremos, por último, en conocimiento de la cantidad r que buscamos (*).

3.° *Dividir la circunferencia en* 17 *partes iguales.*—Para la raiz primitiva $g = 3$ del número 17, tenemos:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15. *Indices.*

1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6. *Números.*

Descompongamos en cuatro factores $p - 1 = 16 = 2 \cdot 2 \cdot 2 \cdot 2$.

(*) El lector que desee conocer al pormenor este asunto puede consultar, ademas de la obra de GAUSS, la especial de BACHMANN, *Die Lehre von der Kreistheilung;* y el *Algebra superior* de SERRET, 3.ª edicion, t. 2.°, cap. III.

Formemos primeramente los dos períodos η_0, η_1, de ocho términos:

$$\eta_0 = [1] + [9] + [13] + [15] + [16] + [8] + [4] + [2]$$

$$\eta_1 = [3] + [10] + [5] + [11] + [14] + [7] + [12] + [6]$$

Estos períodos son raices de la ecuacion de segundo grado:

$$x^2 - (\eta_0 + \eta_1) x + \eta_0 \eta_1 = 0.$$

La suma de los dos períodos es igual á la de todas las raices de la ecuacion

$$x^{16} + x^{15} + x^{14} + \ldots\ldots + x^2 + x + 1 = 0,$$

esto es, igual á -1: el producto (129)

$$\eta_0 \eta_1 = 4(\eta_0 + \eta_1) = -4.$$

Sustituyendo, la primera ecuacion se convierte en esta otra:

$$x^2 + x - 4 = 0,$$

cuyas dos raices son:

$$\eta_0 = \frac{-1 + \sqrt{17}}{2} \quad \text{y} \quad \eta_1 = \frac{-1 - \sqrt{17}}{2};$$

las cuales hemos establecido desde luego que representan respectivamente los valores de los períodos η_0 y η_1 en el supuesto de que la raiz r de la ecuacion del círculo para este caso haya sido elegida convenientemente.

Descompongamos ahora cada uno de los períodos ya determinados, de ocho términos, en dos de á cuatro términos, á saber:

$$\eta_0 \begin{cases} \eta'_0 = [1]+[13]+[16]+[4] \\ \eta'_2 = [9]+[15]+[8]+[2] \end{cases} \qquad \eta_1 \begin{cases} \eta'_1 = [3]+[5]+[14]+[12] \\ \eta'_3 = [10]+[11]+[7]+[6] \end{cases}$$

Los períodos η'_0, η'_2 que componen el η_0, así como los η'_1, η'_3 que componen el η_1, satisfacen respectivamente á dos ecuaciones de segundo grado, cuyos coeficientes no son en verdad números racionales, pero pueden ser racionalmente expresados en funcion de los períodos primitivos η_0 y η_1. Dichas dos ecuaciones son:

$$x^2 - (\eta'_0 + \eta'_2)\, x + \eta'_0\, \eta'_2 = 0, \quad x^2 - (\eta'_1 + \eta'_3)\, x + \eta'_1\, \eta'_3 = 0,$$

ó bien estas otras equivalentes:

$$x^2 - \eta_0 x - 1 = 0 \qquad x^2 - \eta_1 x - 1 = 0,$$

y sus raices respectivas:

$$x = \frac{\eta_0}{2} \pm \sqrt{\frac{\eta_0^2}{4} + 1}, \qquad x = \frac{\eta_1}{2} \pm \sqrt{\frac{\eta_1^2}{4} + 1}.$$

Establezcamos arbitrariamente las igualdades,

$$\eta'_0 = \frac{\eta_0}{2} + \sqrt{\frac{\eta_0^2}{4} + 1}, \qquad \eta'_2 = \frac{\eta_0}{2} - \sqrt{\frac{\eta_0^2}{4} + 1};$$

para discernir ahora qué clase de relacion guardan los otros dos períodos η'_1 y η'_3 con las raices de la segunda ecuacion, emplearemos el

medio que Gauss explica (*). Fórmese, segun el procedimiento tantas veces recordado (129), el producto $(\eta'_0 - \eta'_2)(\eta'_1 - \eta'_3)$, y hallaremos la ecuacion:

$$(\eta'_0 - \eta'_2)(\eta'_1 - \eta'_3) = 2(\eta_0 - \eta_1),$$

ó bien, despues de sencillas sustituciones, la siguiente:

$$+\sqrt{\frac{\eta_0^2}{4} + 1} \cdot (\eta'_1 - \eta'_3) = +\sqrt{17};$$

de la cual se desprende que la diferencia $\eta'_1 - \eta'_3$ debe ser positiva, y para esto es necesario que:

$$\eta'_1 = \frac{\eta_1}{2} + \sqrt{\frac{\eta_1^2}{4} + 1} \quad \text{y} \quad \eta'_3 = \frac{\eta_1}{2} - \sqrt{\frac{\eta_1^2}{4} + 1}$$

Descompongamos nuevamente cada uno de los cuatro períodos η, de cuatro términos, en dos períodos bimembres, y tendremos:

$$\eta'_0 \begin{cases} \eta_0'' = [1] + [16] \\ \eta_4'' = [13] + [4] \end{cases} \qquad \eta'_1 \begin{cases} \eta_1'' = [3] + [14] \\ \eta_5'' = [5] + [12] \end{cases}$$

$$\eta'_2 \begin{cases} \eta_2'' = [9] + [8] \\ \eta_6'' = [15] + [2] \end{cases} \qquad \eta'_3 \begin{cases} \eta_3'' = [10] + [7] \\ \eta_7'' = [11] + [6] \end{cases}$$

Cada dos períodos η'', que componen uno de los η', sabemos que son raices de una ecuacion de segundo grado, cuyos coeficientes pueden ser expresados racionalmente en funcion de estos períodos η'. Consideraremos solamente, y basta para nuestro propósito, la ecuacion

(*) D. A., §. 352.

de segundo grado, cuyas raices son los dos períodos η_0'' y η_4'', ó la ecuacion

$$x^2 - \left(\eta_0'' + \eta_4''\right) x + \eta_0''.\eta_4'' = 0,$$

equivalente á

$$x^2 - \eta'_0 x + \eta'_1 = 0,$$

de la cual se deducen los valores de sus raices x, pudiéndose establecer la igualdad

$$\eta_0'' = \frac{\eta'_0}{2} + \sqrt{\frac{\eta_0''^2}{4} - \eta'_1}.$$

Prosiguiendo el mismo método, la ecuacion que inmediatamente debemos resolver es, por último, aquella que tiene por raices las dos potencias de la raiz r de la ecuacion del círculo, que componen el período η_0'', ó la ecuacion de segundo grado

$$x^2 - \left(r + r^{16}\right) x + r \,.\, r^{16} = 0,$$

ó su equivalente

$$x^2 - \eta_0'' x + 1 = 0,$$

de la cual se deduce el valor de la misma raiz r, á saber:

$$r = \frac{\eta_0''}{2} + \sqrt{\frac{\eta_0''^2}{4} - 1} = cos.\frac{2k\pi}{17} + i\,sen.\frac{2k\pi}{17}.$$

Construccion.—Ante todo conviene recordar que, segun sus valores correspondientes, antes expresados, el período η_0 es positivo, el η_1 negativo, y los η_0', η_1', η_0'' positivos; siendo el último

$$\eta_0'' = 2\,cos.\frac{2k\pi}{17}.$$

Dicho esto, en la circunferencia que se trata de dividir en 17 partes, y cuyo radio es la unidad, trácense dos diámetros perpendiculares entre sí, AB y CD; en los puntos A y D las tangentes que se cortan en el punto S, y tómese la distancia $AE = \frac{1}{4}AS$. En el triángulo rectángulo EAO tenemos:

$$OE = \sqrt{AO^2 + AE^2} = \sqrt{1 + \frac{1}{16}} = \frac{1}{4}\sqrt{17}.$$

Haciendo centro en E describiremos una circunferencia con el radio OE, que cortará á la línea AS en los puntos F y F'; y entónces:

$$AF = EF - EA = OE - EA = \frac{1}{4}\sqrt{17} - \frac{1}{4} = \frac{\sqrt{17}-1}{4} = \frac{\eta_0}{2}$$

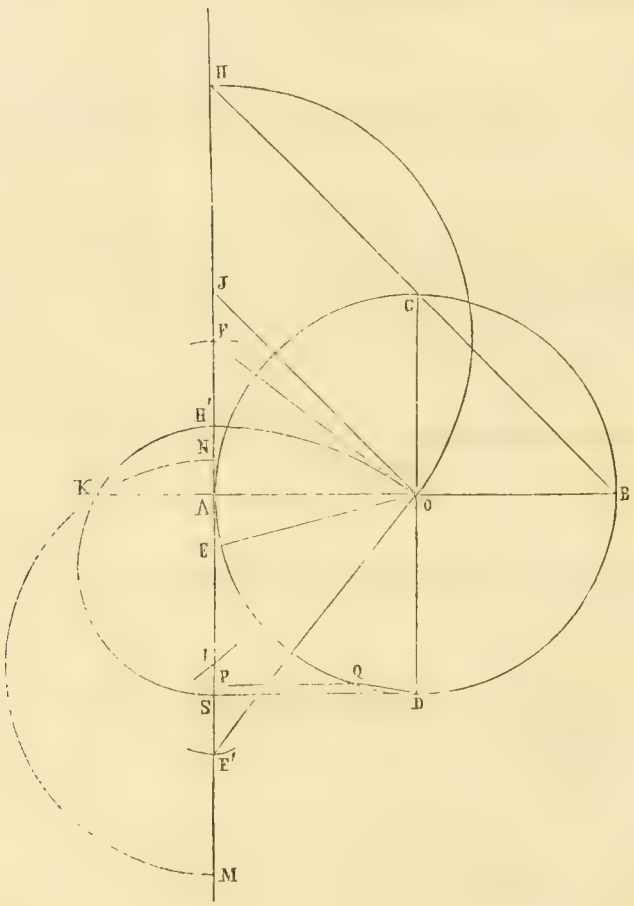
$$AF' = EF' + EA = OE + EA = \frac{1}{4}\sqrt{17} + \frac{1}{4} = \frac{\sqrt{17}+1}{4} = -\frac{\eta_1}{2}.$$

Con estos datos, de los triángulos rectángulos FAO y $F'AO$, se deducen los siguientes:

$$OF = \sqrt{AO^2 + AF^2} = \sqrt{\frac{\eta_0^2}{4} + 1}$$

$$OF' = \sqrt{AO^2 + AF'^2} = \sqrt{\frac{\eta_1^2}{4} + 1}.$$

Alrededor del punto F, con el radio FO, y al rededor del punto F', con el $F'O$, tracemos dos circunferencias que cortarán respectivamente á la línea AS en los puntos H y H'; y dividamos el frag-



mento AH, en dos partes iguales, mediante la paralela OJ á la recta BH. De esta nueva construccion resulta:

$$AH = FH + FA = FO + FA = \frac{r_0}{2} + \sqrt{\frac{r_0^2}{4} + 1} = r'_0$$

$$AH' = F'H' - F'A = F'O - F'A = \frac{r_1}{2} + \sqrt{\frac{r_1^2}{4} + 1} = r'_1$$

$$AJ = \frac{1}{2} AH = \frac{r'_0}{2}$$

Sobre la porcion $H'S$ como diámetro, describamos una semicircunferencia, y prolonguemos AB hasta su interseccion K, con esta misma línea; con lo cual

$$AK^2 = AH' . AS = r'_1 .$$

Desde el punto K, como centro, tracemos ahora una circunferencia con el radio AJ, y con este mismo radio, desde el punto L en que aquélla corta á la recta AS, el semicírculo MKN; y resultará entónces que:

$$AK^2 = AM . AN:$$

y, por consecuencia,

$$AM . AN = r'_1 ,$$

al mismo tiempo que

$$AM + AN = 2 . AJ = r'_0 .$$

Lo cual prueba que AM y AN son las raices de la ecuacion de segundo grado

$$x^2 - r'_0 x + r'_1 = 0 ,$$

y la mayor, $AM = \eta_0'' = 2\,cos.\,\frac{2k\pi}{17}$. Señalando el medio de esta distancia AM por el punto P, será el trozo $AP = \frac{1}{2}\eta_0'' = cos.\,\frac{2k\pi}{17}$. Conocido el coseno del arco que buscamos, es evidente que el punto de interseccion Q, de la paralela PQ al diámetro AB, de la circunferencia dada, con esta circunferencia, será un vértice del polígono de 17 lados, y uno de estos lados la cuerda QD, cuyo arco tiene efectivamente por coseno la distancia AP.

PARTE TERCERA.

TEORÍA DE LAS FORMAS CUADRÁTICAS.

CAPITULO I.

De la trasformacion y equivalencia de las formas cuadráticas en general.

El objeto de nuestro estudio en esta tercera y última parte, á la cual sirven principalmente de lemas las dos anteriores, es ya en toda su pureza el de la teoría de los números, á saber: la representacion de éstos por *formas* (38), limitándonos, como es consiguiente (102), á las de segundo grado ó cuadráticas.

Pero tal representacion ó construccion de los números depende íntimamente de la equivalencia de las mismas *formas*, segun más adelante demostraremos; y así, para proceder con órden, siguiendo á Gauss (*) y con más exactitud aún á su ilustrado comentador Dedekind (**), expondremos desde luego la doctrina general de dicha equivalencia, con sus antecedentes precisos é indispensables.

134.—*Preliminares.*

Las expresiones analíticas de que vamos á tratar exclusivamente son las *homogéneas, binarias* y *cuadráticas*, de la forma

$$a x^2 + 2 b x y + c y^2:$$

(*) D. A., Sectio quinta.

(**) Dirichlet, Zahlentheorie, cap. IV.

en la cual representan las letras a, b, c números enteros, determinados; y las x é y números enteros tambien, pero indeterminados y variables.

Nótase desde luego en la forma escrita, completamente definida, que el coeficiente del producto xy, de las dos variables, se halla expresado por el número par $2b$; mas, si bien este modo de expresion parece en cierto sentido particular, tiene la ventaja de facilitar los cálculos, como veremos, y en realidad no envuelve limitacion alguna; porque una forma cualquiera, en la cual el coeficiente del producto de sus dos variables fuese impar, se reduciria á la propuesta, multiplicándola por 2; y entónces de las propiedades de la trasformada se deducirian sencillamente las referentes á la primitiva.

Sin embargo de ser $2b$ el coeficiente del segundo término de la forma en cuestion, llámase a el *primer coeficiente*, b (y no $2b$) el *segundo*, y c el *tercero*, por el órden en que están colocados; designándose ademas los dos, a y c, con el nombre de *extremos*, y el b con el de *medio;* y las dos variables, x é y, respectivamente, con los de *primera* y *segunda.*

Bajo la sola palabra *forma* comprenderemos siempre la cuadrática establecida, y la representaremos brevemente tambien por el símbolo (a, b, c).

De estas formas excluimos todas las que sean susceptibles de ser descompuestas en dos factores lineales, cuyo estudio es fácil y requiere procedimientos distintos esencialmente de los que habremos de emplear en lo sucesivo. Despréndese de tal exclusion que ninguno de los coeficientes extremos de las formas, objeto de nuestras investigaciones, puede ser igual á *cero;* ni tampoco la cantidad $b^2 - ac$ un cuadrado perfecto: pues, si lo fuera, de la igualdad

$$ax^2 + 2bxy + cy^2 = \frac{1}{a}\left\{(ax + by)^2 - (b^2 - ac)y^2\right\}$$

se deduciria esta otra:

$$ax^2 + 2bxy + cy^2 = \frac{1}{a}\left\{ax + (b + \sqrt{b^2 - ac})\,y\right\} \times \left\{ax + (b - \sqrt{b^2 - ac})\,y\right\};$$

esto es, la descomposicion de la forma en dos factores lineales, contra lo terminantemente establecido. La cantidad $b^2 - ac$, de la que dependen principalmente, segun veremos en lo sucesivo, las propiedades de la forma (a, b, c), se llama *determinante* de esta forma, y se representa sencillamente por su inicial, la letra D. Con esta notacion podemos resumir lo anterior, diciendo que vamos á tratar en adelante exclusivamente de las formas, cuya determinante D, no sea un cuadrado perfecto, ó en las que $\sqrt{D}$ sea siempre un número irracional.

135.—*Trasformacion ó sustitucion simple: propia é impropia.*

Entre las variables x é y de la forma cuadrática (a, b, c), y otras dos nuevas variables x' é y', establezcamos las relaciones lineales

$$\begin{aligned} x &= \alpha x' + \beta y' \\ y &= \gamma x' + \delta y' \end{aligned} \qquad (1)$$

en las cuales $\alpha, \beta, \gamma, \delta$ representan números enteros, determinados. Introduciendo los valores (1) de las variables x é y en la forma (a, b, c), se convierte ésta en la (a', b', c'), cuyos coeficientes están enlazados con los de la forma primitiva y los números $\alpha, \beta, \gamma, \delta$, como se expresa en las ecuaciones siguientes:

$$\begin{aligned} a' &= a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \\ b' &= a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta \\ c' &= a\beta^2 + 2b\beta\delta + c\delta^2 \end{aligned} \qquad (2).$$

La dependencia así establecida entre la forma $(a,b,c) = ax^2 + 2bxy + cy^2$, y la nueva $(a', b', c') = a'x'^2 + 2b'x'y' + c'y'^2$, se expresa diciendo que la primera (a, b, c), por la *trasformacion* ó *sustitucion lineal* (1), se

convierte en la segunda (a', b', c'); designándose los números $\alpha, \beta, \gamma, \delta$ respectivamente con los nombres de *primero*, *segundo*, *tercero* y *cuarto coeficientes* de sustitucion.

Como la eleccion de las letras para representar las variables es enteramente arbitraria, y la naturaleza de las formas y de las sustituciones depende exclusivamente de los coeficientes, podemos brevemente decir que la forma (a, b, c), por la sustitucion $(\alpha, \beta, \gamma, \delta)$ ó $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$, se convierte en la forma (a', b', c'); y este modo de expresion supone implícita y necesariamente que se verifican las ecuaciones (2). Para fijar bien las ideas en este punto, cambiando la colocacion respectiva de los coeficientes de las formas y los de sustitucion, añadiremos, por ejemplo, que simultáneamente:

(a, b, c) por la sustitucion $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ se convierte en la (a', b', c')

(a, b, c) ..... $\begin{pmatrix} \beta, & \alpha \\ \delta, & \gamma \end{pmatrix}$ ..... (c', b', a')

(c, b, a) ..... $\begin{pmatrix} \gamma, & \delta \\ \alpha, & \beta \end{pmatrix}$ ..... (a', b', c')

(c, b, a) ..... $\begin{pmatrix} \delta, & \gamma \\ \beta, & \alpha \end{pmatrix}$ ..... (c', b', a')

trasformaciones muy fáciles de comprender, atendiendo á las citadas ecuaciones (2).

Teniendo ahora en cuenta la representacion de los números por las formas, comprendemos en seguida que todo número representado por la trasformada (a', b', c'), lo estará tambien por la primitiva (a, b, c); pues, admitiendo que aquélla represente en efecto el número m, para los valores determinados r', s' de sus dos variables x', y', de la sustitucion entónces cierta,

$$r = \alpha r' + \beta s'$$

$$s = \gamma r' + \delta s',$$

resultaria que dicho número m, estaria tambien representado por la forma (a, b, c) para los valores especiales de sus variables $x=r$, $y=s$. Segun esto podemos decir tambien que la forma (a, b, c) *contiene* á la (a', b', c') ó, más claramente, que la forma (a', b', c') *se halla contenida* en la (a, b, c); porque todos los números representados por la (a', b', c') se encuentran comprendidos entre los representados por la (a, b, c).

Conocidas las relaciones entre los coeficientes de las formas (a, b, c) y $(a', b', c',)$, nada más fácil que hallar la que exista entre sus respectivas determinantes; pues para ello basta sustituir en la expresion de la determinante

$$D' = b'^2 - a'c',$$

por a', b', c', sus valores (2). Efectuándolo así se obtiene, despues de sencillas reducciones, la interesante relacion

$$D' = (\alpha\delta - \beta\gamma)^2 D;$$

de la cual se desprende que *la nueva determinante es igual á la antigua multiplicada por un cuadrado;* y, en consecuencia, que *una y otra tienen el mismo signo.*

Ahora bien, para que las ecuaciones (1) expresen realmente el concepto que les hemos atribuido, es indispensable que sean solubles respecto de las variables x', y', y para ésto que la cantidad $\alpha\delta - \beta\gamma$, que se llama la *determinante de sustitucion*, sea diferente de cero. Desde luego excluimos de nuestro estudio todas las sustituciones cuya determinante sea cero; pero todavía tenemos que hacer reflexiones más importantes.

Si la determinante de sustitucion $\alpha\delta - \beta\gamma$, ha de tener un valor diferente de cero, habrá de ser necesariamente *positiva* ó *negativa;* la sustitucion correspondiente se llamará *propia* en el primer caso, é *impropia* en el segundo; y se dirá tambien que una forma (a', b', c') está *propia* ó *impropiamente* contenida en otra (a, b, c) segun que la sustitucion $\begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix}$ por la cual se convierte esta última en la primera, sea *propia* ó *impropia.*

Preciso es añadir, para desvanecer dudas y evitar equivocaciones,

que una forma puede contener á otra de los dos modos: propia é impropiamente; pues ocurre con frecuencia que una forma, mediante una sustitucion *propia*, y otra *impropia*, se convierte en la misma. Así sucede con la forma (3, 13, 18), por ejemplo, la cual, por la sustitucion propia $\begin{pmatrix} +1, & 0 \\ -1, & +1 \end{pmatrix}$, y por la impropia $\begin{pmatrix} +1, & +2 \\ -1, & +3 \end{pmatrix}$, se convierte en la misma $(-5, -5, 18)$; y contiene á ésta, por lo tanto, *propia* é *impropiamente*.

Dos sustituciones se denominan *homogéneas* cuando las dos son propias, ó las dos son impropias; y *heterogéneas* cuando una de ellas es propia, é impropia la otra.

136.—*Trasformacion ó sustitucion compuesta: propia é impropia.*

Conservando la notacion anterior, supongamos ahora que la forma

$$(a', b', c') = a' x'^2 + 2 b' x' y' + c' y'^2,$$

mediante la nueva sustitucion

$$x' = \alpha' x'' + \beta' y''$$
$$y' = \gamma' x'' + \delta' y'',$$

se convierte en esta otra:

$$(a'', b'', c'') = a'' x''^2 + 2 b'' x'' y'' + c'' y''^2.$$

Es evidente que la primera forma (a, b, c) se convertirá en la tercera (a'', b'', c''), mediante la sustitucion

$$x = \alpha (\alpha' x'' + \beta' y'') + \beta (\gamma' x'' + \delta' y'')$$
$$y = \gamma (\alpha' x'' + \beta' y'') + \delta (\gamma' x' + \delta' y'')$$

ó su igual

$$x = (\alpha\alpha' + \beta\gamma')\,x'' + (\alpha\beta' + \beta\delta')\,y''$$

$$y = (\gamma\alpha' + \delta\gamma')\,x'' + (\gamma\beta' + \delta\delta')\,y''$$

De donde se deduce que, *si una forma contiene á otra, y ésta á otra tercera, la primera contendrá tambien á la última.*

Para saber ahora de qué modo contiene la primera forma á la tercera, deberemos inquirir qué signo tendrá la determinante de la sustitucion última, por la cual se trasforma la una en la otra. Esta determinante es, como ya dijimos,

$$(\alpha\alpha' + \beta\gamma')\,(\gamma\beta' + \delta\delta') - (\alpha\beta' + \beta\delta')\,(\gamma\alpha' + \delta\gamma');$$

representándola por ε, y llamando D'' la determinante de la tercera forma (a'', b'', c''), será, segun manifestamos en el párrafo anterior,

$$D'' = \varepsilon^2 D.$$

Mas tambien, por igual razon, se verifican las igualdades

$$D' = (\alpha\delta - \beta\gamma)^2 D, \qquad D'' = (\alpha'\delta' - \beta'\gamma')^2 D'$$

de las cuales se desprende esta otra:

$$D'' = (\alpha\delta - \beta\gamma)^2 \times (\alpha'\delta' - \beta'\gamma')^2 D,$$

que cotejada con la precedente, y teniendo en cuenta que las determinantes D, D', D'' no pueden ser nulas, da para ε el valor

$$\varepsilon = (\alpha\delta - \beta\gamma)\,(\alpha'\delta' - \beta'\gamma').$$

Es decir que la determinante de la sustitucion, por la cual se convierte la primera forma en la tercera, es igual al producto de las determinantes de las dos sustituciones intermediarias; y de aquí resulta que

la *primera contendrá propia ó impropiamente á la tercera, segun que las dos sustituciones, de la primera en la segunda, y de ésta en la tercera, sean homogéneas ó heterogéneas.*

Si prosiguiendo, admitimos que la forma tercera contenga á otra, y ésta á su vez se trasforme en una quinta, etc., la ley anterior puede generalizarse de este modo:

En una série de formas, cada una de las cuales contenga á su inmediata posterior, la primera contendrá á la última, propia ó impropiamente, segun que el número de las sustituciones intermediarias sucesivas, impropias, sea par ó impar.

La sustitucion por la cual se convierte una forma en otra que no sea su inmediata, se llama *compuesta;* y el enlace entre esta sustitucion compuesta y las dos simples componentes, refiriéndonos á tres formas nada más, segun se desprende de las fórmulas arriba escritas, se expresa como sigue:

$$\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix}\ \begin{pmatrix}\alpha', \beta'\\ \gamma', \delta'\end{pmatrix} = \begin{pmatrix}\alpha\alpha' + \beta\gamma', \ \alpha\beta' + \beta\delta'\\ \gamma\alpha' + \delta\gamma', \ \gamma\beta' + \delta\delta'\end{pmatrix}$$

En general se comprende que no podrá invertirse el órden de las sustituciones simples sin que se altere tambien la sustitucion compuesta, resultante. Así vemos, por ejemplo, que las sustituciones parciales $\begin{pmatrix}+1, 0\\ -1, 1\end{pmatrix}$, $\begin{pmatrix}+1, +2\\ -1, -3\end{pmatrix}$ producen, en un órden, la compuesta

$$\begin{pmatrix}+1, 0\\ -1, 1\end{pmatrix}\ \begin{pmatrix}+1, +2\\ -1, -3\end{pmatrix} = \begin{pmatrix}+1, +2\\ -2, -5\end{pmatrix},$$

y, en el órden inverso, esta otra:

$$\begin{pmatrix}+1, +2\\ -1, -3\end{pmatrix}\ \begin{pmatrix}+1, 0\\ -1, 1\end{pmatrix} = \begin{pmatrix}-1, +2\\ +2, -3\end{pmatrix}.$$

Por el contrario, siendo tres las sustituciones sucesivas, S, S', S'',

el mismo resultado se obtiene juntando la primera S, con la segunda S', y el compuesto SS' de ambas, con la tercera S''; que uniendo la segunda S', con la tercera S'', y el compuesto $S'S''$ de las dos despues con la primera S; en signos:

$$(SS')\,S'' = S\,(S'\,S'')$$

Y esta relacion se deduce inmediatamente del fondo de la composicion misma; pues, siendo (x, y), (x', y'), (x'', y'') (x''', y'''), las variables sucesivas, en las expresiones de x é y en funcion de x''' é y''', es lo mismo que figuren como intermedias las (x'', y'') que las (x', y').

Conviene ademas notar que la sustitucion $\begin{pmatrix} 1, 0 \\ 0, 1 \end{pmatrix}$, cuya determinante es la unidad, puede suprimirse de toda composicion, puesto que en nada la altera.

Y, finalmente, con estos nuevos signos, la ley anterior puede enunciarse como sigue: *la sustitucion* $SS'S''$ ....., *compuesta de las sustituciones* S, S', S'', ... *será propia ó impropia, segun que el número de estas sustituciones parciales, impropias, sea par ó impar.*

137.—*Equivalencia de las formas: propia é impropia.*

---

a–) Hasta ahora sólo hemos admitido que una forma se convierta en otra; pero es muy interesante saber si esta última podrá á su vez convertirse en la primera; porque de ser así, el sistema de los números por una de ellas representado, seria idéntico al sistema de los números representados por la otra.

Dos formas que mútuamente se contengan se llaman *equivalentes*. Veamos, pues, cuáles son las condiciones necesarias y suficientes de tal equivalencia.

Desde luego, aplicando la definicion de dos formas equivalentes á las expresiones de las determinantes que figuran en los párrafos anteriores, deducimos que los cocientes ó razones $D' : D$, y $D : D'$ deben ser números enteros, cuadrados, y, de consiguiente positivos; y para que ésto

se verifique es indispensable que D y D' sean iguales; de lo cual se desprende que la condicion *necesaria* para que dos formas sean equivalentes, es que sus determinantes, D y D', sean iguales.

Mas esta condicion no es *suficiente* para calificar por ella sola de equivalentes á dos formas cualesquiera; para poder afirmar que lo son, es preciso saber ademas que una de ellas contiene á la otra. En efecto, admitiendo que las dos formas (a, b, c) y (a', b', c') tienen iguales determinantes, y que la primera se trasforma en la segunda, por la sustitucion

$$x = \alpha x' + \beta y'$$

$$y = \gamma x' + \delta y',$$

de la relacion ya conocida

$$D' = (\alpha\delta - \beta\gamma)^2 D,$$

por ser ahora $D = D'$, se desprende esta otra:

$$\alpha\delta - \beta\gamma = \pm 1.$$

Designando por ε, para mayor brevedad, esta última, y despejando las variables (x', y') en la sustitucion antes escrita, resulta la siguiente:

$$x' = +\varepsilon\delta x - \varepsilon\beta y$$

$$y' = -\varepsilon\gamma x + \varepsilon\alpha y;$$

y, como por esta sustitucion, cuyos coeficientes son enteros, se convierte realmente, á su vez, la forma segunda (a', b', c'), en la primera (a, b, c), dichas dos formas son equivalentes.

Las sustituciones que preceden,

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} +\varepsilon\delta, & -\varepsilon\beta \\ -\varepsilon\gamma, & +\varepsilon\alpha \end{pmatrix},$$

se llaman cada una de ellas *inversa* de la otra; y, siendo la sustitucion

compuesta de ambas igual á la $\begin{pmatrix} 1 , 0 \\ 0 , 1 \end{pmatrix}$, cuya determinante es positiva, conclúyese que aquellas dos componentes serán al mismo tiempo propias, ó impropias. Segun ocurra lo primero, ó lo segundo, así se dirá que las dos formas propuestas son *propia*, ó *impropiamente equivalentes*.

Demostrado ya que, si dos formas son equivalentes, la una se convierte en la otra siempre por una sustitucion $\begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix}$, cuya determinante es $\alpha\delta - \beta\gamma = \pm 1$, podemos afirmar recíprocamente: que, mediante toda sustitucion de esta especie, se trasformará tambien una forma cualquiera en otra equivalente; pues tal sustitucion exije que las determinantes de las dos formas sean iguales; y así queda de un modo claro establecida la condicion *necesaria* y *suficiente* para la equivalencia de dos formas.

De la definicion de esta palabra se deduce inmediatamente que toda forma es en el sentido propio equivalente á sí misma; puesto que se convierte en sí misma por la sustitucion

$$\begin{aligned} x &= x' + 0\,y' \\ y &= 0\,x' + y' \end{aligned} \qquad \text{ó} \qquad \begin{pmatrix} 1 , 0 \\ 0 , 1 \end{pmatrix}$$

cuya determinante es, en efecto, la unidad positiva. Mas este corolario es un caso particular de otra proposicion más amplia, á saber:

Siempre que dos formas (a, b, c), (a, b', c'), *de igual determinante, tengan el mismo primer coeficiente* a, *y sean congruentes entre sí* (*mod.* a) *sus coeficientes medios* b, b', *en cuyo caso* $b' = \beta a + b$, *serán propiamente equivalentes; y la primera se trasformará en la segunda mediante la sustitucion propia* $\begin{pmatrix} 1, \beta \\ 0, 1 \end{pmatrix}$.

Dos formas (a, b, c), $(a, -b, c)$, que sólo se diferencian en el signo de sus coeficientes medios, se llaman *opuestas*, y son *impropiamente* equivalentes; pues la una se convierte en la otra por la sustitucion impropia

$$\begin{aligned} x &= x' + 0.y' \\ y &= 0.x' - y' \end{aligned} \qquad \text{ó} \qquad \begin{pmatrix} 1 , & 0 \\ 0 , & -1 \end{pmatrix}.$$

Dos formas (a, b, c) y (c, b, a) que constan de los mismos coeficientes, aunque en órden inverso, se llaman *socias*, y tambien son *impropiamente* equivalentes; puesto que una de ellas se trasforma en la otra mediante la sustitucion impropia

$$\begin{aligned} x &= 0.x' + \quad y' \\ y &= \quad x' + 0.y' \end{aligned} \qquad \text{ó} \qquad \begin{pmatrix} 0, & 1 \\ 1, & 0 \end{pmatrix}.$$

De estas dos sustituciones simples, *impropias*, resulta la compuesta

$$\begin{aligned} x &= (0.1 + 0.1)\, x'' + (1.1 + 0.0)\, y'' \\ y &= (0.0 - 1.1)\, x'' + (0.1 - 1.0)\, y'' \end{aligned} \qquad \text{ó} \qquad \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}$$

que es *propia*, mediante la cual se convierten una en otra, las formas (a, b, c) y $(c, -b, a)$, siendo las dos, en consecuencia, *propiamente* equivalentes.

Más interesantes aún para lo sucesivo que las precedentes son las formas que se denominan *contíguas*. Dos formas de esta especie, $\varphi = (a, b, a')$, $\varphi' = (a', b', a'')$, están caracterizadas: 1.° por tener la misma determinante; 2.° por ser el último coeficiente a', de una de ellas, igual al primero de la otra; 3.° por ser la suma de sus coeficientes medios, $b + b'$, divisible por su coeficiente comun, a'.

Las formas contíguas son propiamente equivalentes. En efecto, desde luego la forma (a, b, a'), por la sustitucion propia $\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$, se convierte en otra equivalente á ella, cuyos coeficientes son:

$$a',\ b' = -b - a'\delta, \quad a'' = a' + 2b\delta + a'\delta^2.$$

Pero los valores de estos coeficientes dependen de los que figuran en la sustitucion empleada: luego siempre que las formas φ y φ' tengan las propiedades arriba escritas, y se verifique la ecuacion $b' + b = -a'\delta$, de la cual se desprende el valor de δ, la forma φ, mediante dicha sustitucion $\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$, se trasformará siempre en otra equivalente á ella, é idéntica á la φ'.

El motivo de fijarnos en las sustituciones de la forma $\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$ se funda en que, como veremos, se componen de ellas todas las demás.

Advertiremos, por último, que cuando se quiere especificar aún más el concepto de las formas contíguas (a, b, a'), (a', b', a''), se dice que la primera es *contígua* por la primera parte, ó *por la izquierda*, de la segunda; y ésta, contígua por la última parte, ó *por la derecha*, de la primera.

b–) Hasta aquí hemos hablado de formas propia, ó impropiamente equivalentes, esto es, equivalentes de un solo modo; pero tambien existen formas equivalentes de los dos modos, es decir, propia é impropiamente equivalentes. En este caso se encuentran, como ya indicamos (135), las dos formas (3, 13, 18) y (—5, —5, 18), la primera de las cuales se convierte en la segunda, mediante la sustitucion propia $\begin{pmatrix} +1, & 0 \\ -1, & 1 \end{pmatrix}$, y la impropia $\begin{pmatrix} +1, & +2 \\ -1, & -3 \end{pmatrix}$; y, recíprocamente: la segunda en la primera, por las sustituciones inversas respectivamente $\begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix}$, y $\begin{pmatrix} +3, & +2 \\ -1, & -1 \end{pmatrix}$.

Demos ahora por sentado, en general, que la forma (a, b, c), por las dos sustituciones

$$\begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix} (propia), \text{ y } \begin{pmatrix} \alpha'', & \beta'' \\ \gamma'', & \delta'' \end{pmatrix} (impropia),$$

se convierte sucesivamente en la (a', b', c'): esta última se convertirá á su vez en la primera, mediante las dos sustituciones, inversas respectivamente de las anteriores,

$$\begin{pmatrix} +\delta', & -\beta' \\ -\gamma', & +\alpha' \end{pmatrix} (propia), \text{ y } \begin{pmatrix} -\delta'', & +\beta'' \\ +\gamma'', & -\alpha'' \end{pmatrix} (impropia),$$

si las dos formas (a, b, c) y (a', b', c') han de ser equivalentes. Y de

ésto resulta que la forma (a, b, c) tornará en sí misma por las dos sustituciones compuestas, y necesariamente impropias,

$$\begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix} \begin{pmatrix} -\delta'', & +\beta'' \\ +\gamma'', & -\alpha'' \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} \alpha'', & \beta'' \\ \gamma'', & \delta'' \end{pmatrix} \begin{pmatrix} +\delta', & -\beta' \\ -\gamma', & +\alpha' \end{pmatrix};$$

y lo mismo sucederá con la otra forma. Luego:

Si dos formas son propia é impropiamente equivalentes, cada una de ellas es impropiamente equivalente á sí misma.

En el ejemplo citado anteriormente se ve confirmada esta ley: la forma (3, 13, 18) se convierte en sí misma por las dos sustituciones compuestas, impropias:

$$\begin{pmatrix} +1, & 0 \\ -1, & 1 \end{pmatrix} \begin{pmatrix} +3, & +2 \\ -1, & -1 \end{pmatrix} = \begin{pmatrix} +3, & +2 \\ -4, & -3 \end{pmatrix}$$

$$\begin{pmatrix} +1, & +2 \\ -1, & -3 \end{pmatrix} \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix} = \begin{pmatrix} +3, & +2 \\ -4, & -3 \end{pmatrix}$$

Mas nótase en este ejemplo un hecho particular, á saber: que dos sustituciones, compuestas de modos diferentes son, sin embargo, idénticas; y es necesario inquirir si esto sucede casualmente, ó si es general en todas las sustituciones impropias, por las cuales una forma torna en sí misma. Establezcamos, pues, la igualdad

$$\begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix} \begin{pmatrix} -\delta'', & +\beta'' \\ +\gamma'', & -\alpha'' \end{pmatrix} = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix};$$

de ella se desprende esta otra:

$$\begin{pmatrix} \alpha'', & \beta'' \\ \gamma'', & \delta'' \end{pmatrix} \begin{pmatrix} +\delta', & -\beta' \\ -\gamma', & +\alpha' \end{pmatrix} = \begin{pmatrix} -\delta, & +\beta \\ +\gamma, & -\alpha \end{pmatrix};$$

y las dos serán idénticas en el supuesto de que los coeficientes α y δ

se consideren iguales y de distinto signo. Veamos, por consecuencia, si en toda sustitucion impropia $\begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix}$, por la cual una forma (a, b, c) torna en sí misma, se verifica efectivamente que sean iguales y de signo contrario los coeficientes primero y cuarto. Para esto, sabemos que, si la forma (a, b, c) ha de convertirse en sí misma, por la sustitucion impropia $\begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix}$, es necesario que se verifiquen las tres ecuaciones:

$$a\alpha^2 + (2b\alpha + c\gamma)\gamma = a$$

$$a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b$$

$$\alpha\delta - \beta\gamma = -1.$$

La segunda de éstas, poniendo en ella por $\beta\gamma$ su valor $\alpha\delta + 1$, deducido de la tercera, se trasforma en la siguiente:

$$a\alpha\beta + (2b\alpha + c\gamma)\delta = 0:$$

de la cual y de la primera, por la eliminacion del binomio $(2b\alpha + c\gamma)$ y supresion despues del factor comun a (diferente de cero), se obtiene esta otra:

$$\alpha^2\delta - \delta = \alpha\beta\gamma.$$

Multiplicando la tercera por α, resulta tambien:

$$\alpha^2\delta + \alpha = \alpha\beta\gamma;$$

y de estas dos últimas igualdades se deduce al fin que realmente es $\delta = -\alpha$.

c-) Síguese de lo dicho que toda sustitucion impropia, por la cual una forma (a, b, c) se convierte en sí misma, habrá de tener precisamente la expresion $\begin{pmatrix} \alpha, +\beta \\ \gamma, -\alpha \end{pmatrix}$ y su determinante será, por lo tanto,

$\alpha^2 + \beta\gamma = 1$. Grande interés para nosotros ofrece el estudio del caso particular en que el tercer coeficiente de esa sustitucion, γ, sea cero; pues entónces $\alpha = \pm 1$, y, en consecuencia, $\pm a\beta = 2b$. Toda forma, en la cual sea el duplo del coeficiente medio divisible por el coeficiente primero, se denomina forma *ambígua* (*anceps*). Toda forma ambígua es á su vez del modo impropio equivalente á sí misma; pues una cualquiera de esta especie (a, b, c), en la cual se verifica la condicion consiguiente $2b = a\beta$, se convierte en sí misma por la sustitucion impropia $\begin{pmatrix} 1, +\beta \\ 0, -1 \end{pmatrix}$; y lo mismo acontece con toda forma que sea equivalente á una forma ambigua: tambien es impropiamente equivalente á sí misma. Pero, recíprocamente:

Dada una forma impropiamente equivalente á sí misma, ¿existirá siempre una forma ambígua, tambien equivalente con ella?

La contestacion afirmativa á esta pregunta es de importancia para nuestras ulteriores investigaciones.

Designemos abreviadamente por φ la forma dada que, por la sustitucion impropia $\begin{pmatrix} \alpha, +\beta \\ \gamma, -\alpha \end{pmatrix}$, torna en sí misma. Si en esta sustitucion fuese $\gamma = 0$, la forma misma φ seria *ambígua*, y la cuestion estaba terminada; pero, no verificándose en tal sustitucion la condicion necesaria para que sea ambígua la forma φ, es preciso averiguar si de ella puede deducirse otra sustitucion $\begin{pmatrix} \lambda, \mu \\ \nu, \rho \end{pmatrix}$ *propia*, mediante la cual se convierta dicha forma φ en una forma ambígua ψ; y para decidir que esta forma ψ es ambígua, es indispensable demostrar que torna en sí misma por una sustitucion impropia, cuyo tercer coeficiente sea cero. Ahora bien, convirtiéndose la forma φ en la forma ψ, por la sustitucion propia $\begin{pmatrix} \lambda, \mu \\ \nu, \rho \end{pmatrix}$ cuya determinante es $\lambda\rho - \mu\nu = +1$, tambien se trasformará la segunda forma ψ en la primera φ, mediante la sustitucion inversa de la anterior, y *propia* como ella, $\begin{pmatrix} +\rho, -\mu \\ -\nu, +\lambda \end{pmatrix}$; y dicha forma ψ, por consecuencia, en sí misma, por la sustitucion

evidentemente *impropia*, y compuesta de las tres sustituciones sucesivas:

$$\begin{pmatrix} +\rho, -\mu \\ -\nu, +\lambda \end{pmatrix}, \quad \begin{pmatrix} \alpha, +\beta \\ \gamma, -\alpha \end{pmatrix}, \quad \begin{pmatrix} \lambda, \mu \\ \nu, \rho \end{pmatrix}.$$

Ya sabemos, pues, que la forma ψ torna en sí misma por una sustitucion impropia, ó bien que es impropiamente equivalente á sí misma; nos resta averiguar si el tercer coeficiente de tal sustitucion es igual á cero para calificarla en definitiva de ambígua. Escribamos para esto explícitamente las tres sustituciones componentes de la sustitucion impropia, antes simbólicamente expresada, como sigue:

$$x = \quad \rho x' - \mu y' \qquad x' = \alpha x'' + \beta y'' \qquad x'' = \lambda x''' + \mu y'''$$

$$y = -\nu x' + \lambda y' \qquad y' = \gamma x'' - \alpha y'' \qquad y'' = \nu x''' + \rho y'''$$

Deduciendo de estas ecuaciones los valores de x é y en funcion de x''' é y''', se obtendrá aquella sustitucion compuesta, impropia, tambien de un modo explícito, y veremos que su tercer coeficiente es en realidad:

$$\gamma\lambda^2 - 2\alpha\lambda\nu - \beta\nu^2.$$

Veamos ahora si es posible determinar los dos números, desconocidos aún, λ, ν, que figuran en la última expresion, de modo que ésta se convierta en cero. Multiplicándola por γ, añadiéndole y quitándole $\alpha^2\nu^2$, y teniendo presente que $\alpha^2 + \beta\gamma = 1$, se convierte en la siguiente:

$$(\gamma\lambda + \alpha\nu)^2 - \nu^2;$$

de la cual, despues de igualada con cero, se deduce:

$$\frac{\lambda}{\nu} = \frac{\alpha \pm 1}{\gamma} = \frac{-\beta}{\alpha \pm 1}.$$

Por estas igualdades se determinan efectivamente los números λ y ν; pues, siendo γ diferente de cero, segun al principio supusimos, y aquellos números λ, ν, primos entre sí, por satisfacer á la ecuacion $\lambda\rho - \mu\nu = 1$, los dos términos de la fraccion $(\alpha \pm 1) : \gamma$, despues de reducida á su mínima expresion, serán iguales respectivamente á los de la fraccion $\lambda : \nu$. Hallados así los números λ, ν, podrán determinarse en seguida infinitos pares de valores (71) para ρ y μ que satisfagan á la ecuacion $\lambda\rho - \mu\nu = 1$; quedando, por fin, demostrado que de la sustitucion dada $\begin{pmatrix} \alpha, +\beta \\ \gamma, -\alpha \end{pmatrix}$, puede deducirse otra $\begin{pmatrix} \lambda, \mu \\ \nu, \rho \end{pmatrix}$, por la cual se convierte la forma propuesta φ en una forma realmente ambigua ψ. Luego:

Si una forma es impropiamente equivalente á sí misma, existe siempre otra forma, ambigua, equivalente con ella.

Sea, por ejemplo, la forma $\varphi = (3, 13, 18)$, que por la sustitucion impropia $\begin{pmatrix} +3, +2 \\ -4, -3 \end{pmatrix}$ torna en sí misma. Los coeficientes λ y ν serán determinados por la ecuacion

$$\frac{\lambda}{\nu} = \frac{3 \pm 1}{-4}.$$

Tomando el signo superior en el numerador del segundo miembro, hallamos: $\lambda = \pm 1$, $\nu = \pm 1$; y, por consecuencia, $\rho + \mu = \pm 1$, de la cual, tomando tambien el signo superior, se deduce, por ejemplo, $\rho = 1$, $\mu = 0$. Con este par de valores de ρ y μ, y los dos anteriores de λ y ν, se obtiene la sustitucion $\begin{pmatrix} +1, 0 \\ -1, 1 \end{pmatrix}$, por la cual se convierte la forma dada $(3, 13, 18) = \varphi$ en la anceps $(-5, -5, 18) = \psi$.

Sea dada ahora la forma $(7, 1, -1)$ que se convierte en sí misma por la sustitucion impropia $\begin{pmatrix} +2, +1 \\ -3, -2 \end{pmatrix}$; tendremos:

$$\frac{\lambda}{\nu} = \frac{2 \pm 1}{-3}.$$

Refiriéndonos siempre, como antes, á los signos superiores, se obtienen los coeficientes $\lambda = 1$, $\nu = -1$, $\rho = 1$, $\mu = 0$, de la sustitucion $\begin{pmatrix} +1, 0 \\ -1, 1 \end{pmatrix}$, por la cual se trasforma la forma $(7, 1, -1)$ en la $(4, 2, -1)$ que es ambígua realmente.

CAPITULO II.

De la equivalencia de las formas en particular. Sus dos problemas fundamentales.

138.—*Clasificacion de las formas.—Sistema completo de formas no equivalentes.*

Expuestas las consideraciones generales que preceden sobre la equivalencia de las formas, debemos antes de proseguir nuestro estudio declarar que en lo sucesivo trataremos exclusivamente de la equivalencia *propia*. Así que, mientras explícitamente no digamos lo contrario, cuando hablemos de dos formas equivalentes, se entenderá siempre que existe una sustitucion propia por la cual se convierte una de ellas en la otra; y, recíprocamente: que esta última se trasforma en la primera mediante la sustitucion inversa de la anterior, y, por consecuencia, tambien propia.

Hecha esta advertencia indispensable, el principio que sirve de base á la teoría de las formas, ligada estrechamente con la de la equivalencia, como veremos pronto, y que se desprende del más general, ya demostrado (136), es el siguiente:

Dos formas, equivalentes á otra, son equivalentes entre sí.

Segun este principio, si designamos por f una forma, cuya determinante sea D, y por F el conjunto de todas las formas f, f', f''..... equivalentes con aquella, cada dos de estas formas f', f'', serán tam-

bien equivalentes entre sí; y, por consecuencia, el sistema de todas las formas equivalentes con cualquiera f', de las contenidas en el conjunto F, será idéntico á este conjunto. Este sistema ó conjunto de formas equivalentes entre sí se denomina *clase;* y es evidente que mediante una sola forma, perteneciente á una de estas clases, están completamente determinadas todas las demas que á la misma clase pertenezcan; por cuya razon dicha forma ó individuo se llama *representante* de su clase.

Si consideramos distribuidas todas las formas con igual determinante D, en sus diferentes clases, y de cada una de estas clases elegimos arbitrariamente una forma ó *representante*, constituiremos un *sistema completo de formas no equivalentes* para la determinante D. La propiedad característica de tal sistema completo S, estriba en que toda forma de determinante D, será *siempre* equivalente á una *sola* de las contenidas en dicho sistema S.

139.—*Problemas fundamentales de la equivalencia.—Su relacion íntima con la teoría de las formas.*

Los dos problemas fundamentales en la teoría de la equivalencia son los siguientes:

1.° Averiguar si dos formas dadas, con iguales determinantes, son, ó no son equivalentes; ó bien, si pertenecen, ó no, á la misma clase.

2.° Dadas dos formas equivalentes, hallar todas las sustituciones por las cuales se convierte la una en la otra.

Veamos ahora ya claramente la íntima relacion, varias veces indicada, entre estos dos problemas y la teoría de las formas, ó más particularmente, entre los mismos y la representacion por dichas formas de los números.

Dícese que un número entero m, es *construido*, ó está *representado* por una forma cuadrática (a, b, c), siempre que existan dos números enteros x, y, que verifiquen la ecuacion

$$a x^2 + 2 b x y + c y^2 = m \qquad (1)$$

Cada par (x, y) de los mencionados números se llama una *construccion* del número m por la forma (a, b, c); y es evidente que, en general, habrá para un mismo número diferentes construcciones. Entre todas ellas, sin embargo, sólo tenemos precision de considerar las *propias:* esto es, aquellas construcciones (x, y), en las cuales los *números constructores*, x é y, sean primos relativos. Porque, si no lo fueran, y δ significase entónces su máximo comun divisor, el número m habria de ser necesariamente divisible por δ^2. Estableciendo ahora las igualdades consiguientes $x = x'\,\delta$, $y = y'\,\delta$, $m = m'\,\delta^2$, es evidente que la forma (a, b, c) representará el número m', si los números constructores son x', y'; y, como estos números, primos entre sí, forman una construccion propia, de la cual pueden fácilmente deducirse todas las *impropias,* es inútil tratar de las últimas.

Hecha esta exclusion, estudiemos las condiciones necesarias y suficientes para que un número dado m, pueda ser construido ó representado por una forma dada (a, b, c).

a-) Admitamos que el número m sea representado propiamente por la forma (a, b, c), cuya determinante es $D = b^2 - ac$. Siendo propia la construccion (1) del número m, los números constructores $(x, y,)$ serán primos entre sí; y existirán, por consecuencia, (71), infinitos pares de números (τ_1, ξ), que satisfagan á la ecuacion

$$x\,\tau_1 - y\,\xi = +1 \qquad (2).$$

Pero esta ecuacion es la determinante de la sustitucion propia $\begin{pmatrix} x, & \xi \\ y, & \tau_1 \end{pmatrix}$ que contiene un par cualquiera (τ_1, ξ) de los infinitos, mencionados, y por la cual se convierte la forma (a, b, c) en otra equivalente (137-*a*); y, por consecuencia, con la misma determinante D. Efectuando realmente tal sustitucion, se encuentra que el primer coeficiente de la trasformada, teniendo en cuenta la ecuacion (1), es el mismo número construido m; y que el coeficiente medio es:

$$n = (a\,x + b\,y)\,\xi + (b\,x + c\,y)\,\tau_1 \qquad (3).$$

En cuanto al tercero l, se deduce sencillamente, como m no pue-

de ser cero, del valor de la determinante de la nueva forma, $D=n^2-ml$, y tiene por expresion

$$l = \frac{n^2 - D}{m}.$$

De todo lo cual resulta que la forma (a, b, c), supuesta la construccion (1), se convierte en la equivalente (m, n, l); y, como el tercer coeficiente l, de esta nueva forma, debe ser necesariamente un número entero, y esto exige que $(n^2 - D)$ sea divisible por m, ó que se verifique la congruencia $n^2 \equiv D \pmod{m}$, *D será resto cuadrático de n, ó bien* $z = n$ *una raiz de la congruencia*

$$z^2 \equiv D \pmod{m} \qquad (4).$$

b–) En lugar de los dos números η, ξ, antes elegidos, tomemos otro par η', ξ', que satisfará tambien á la ecuacion (2): la forma (a, b, c) entónces, por la nueva sustitucion $\begin{pmatrix} x, & \xi' \\ y, & \eta' \end{pmatrix}$, se convertirá tambien en otra equivalente (m, n', l'), cuyo coeficiente medio será:

$$n' = (a\,x + b\,y)\,\xi' + (b\,x + c\,y)\,\eta'.$$

Este coeficiente n', es asimismo una raiz, como el n, de la congruencia (4); é interesa mucho conocer la dependencia que entre uno y otro exista. Para esto escribamos las igualdades $x\eta - y\xi = 1 = x\eta' - y\xi'$ que expresan la hipótesis préviamente admitida de que los dos pares de números (η, ξ), (η', ξ') satisfacen á la ecuacion (2): de ellas se desprende esta otra: $x\,(\eta - \eta') = y\,(\xi' - \xi)$; y de aquí, como los números x, y son primos relativos, que $\xi' - \xi$ debe ser divisible por x. Llamando v al cociente de esta division, resultan las fórmulas

$$\xi' = \xi + x\,v \qquad \eta' = \eta + y\,v:$$

las cuales, si v representa un número entero cualquiera, comprende-

rán todas las soluciones de la ecuacion (2); y recíprocamente: á cada valor de v corresponderán dos números (ξ', η'), que satisfarán á dicha ecuacion; y ésto sucederá áun cuando uno de los dos números (x, y), sea igual á cero, y el otro, por consecuencia, igual á ± 1.

Sustituyendo los valores anteriores de ξ' y η' en el de n', y teniendo presentes las ecuaciones (1) y (3), se obtiene el resultado:

$$n' = n + m\,v \qquad \text{ó bien} \qquad n' \equiv n \pmod{m}:$$

del cual se infiere que todas las raices n de la congruencia (4), deducidas, del modo que hemos explicado, de una construccion propia, dada (x, y), del número m por la forma (a, b, c), constituyen los individuos de una clase entera de números congruentes (mod. m), y representan, por lo tanto, una sola raiz. Y es evidente además que cada uno de los individuos de dicha clase aparecerá una sola vez cuando v reciba todos sus valores posibles, esto es: cuando empleemos sucesivamente todas las soluciones (η, ξ) de la ecuacion (2). Así se dice, por consecuencia, que la construccion (x, y) del número m, *pertenece* á la raiz mencionada n (mod. m); pues, mediante el anterior procedimiento, sólo esta raiz n, y no otra alguna, podemos obtener.

Nótase al mismo tiempo que la forma (a, b, c), mediante todas las sustituciones $\begin{pmatrix} x, & \xi \\ y, & \eta \end{pmatrix}$ cuyos coeficientes, primero y tercero, son los números constructores (x, y), se convertirá en infinitas formas equivalentes (m, n, l) que tendrán todas ellas por primer coeficiente el número construido m, y por segundos sucesivamente cada uno de los individuos de una clase entera (mod. m).

b'-) Esta clase de números n (mod. m) puede inmediatamente deducirse de la construccion dada (x, y) sin recurrir á los números (η, ξ). En efecto, resolviendo las ecuaciones (2) y (3), ambas de primer grado respecto de η y ξ, se obtienen las siguientes:

$$m\,\eta = a\,x + (b + n)\,y, \qquad -m\,\xi = (b - n)\,x + c\,y$$

y de éstas, las congruencias:

$$-y\,n \equiv a\,x + b\,y, \qquad x\,n \equiv b\,x + c\,y \pmod{m}$$

que determinan completamente la clase n (mod. m).

Conviene demostrar aquí tambien otra proposicion que habrá de servirnos en lo sucesivo, á saber: *siempre que existan dos números* (x, y) *que satisfagan á las condiciones*

$$a x^2 + 2 b x y + c y^2 = m$$

$$a x + (b + n) y \equiv 0, \qquad (b - n) x + c y \equiv 0 \,(\text{mod. } m),$$

en las cuales m, n, a, b, c *representan números conocidos, siendo siempre* m *diferente de cero, la forma* (a, b, c) *será equivalente á la* (m, n, l). Pues igualando á $m\eta$ y $-m\xi$ respectivamente los primeros miembros de las anteriores congruencias, multiplicando las igualdades resultantes por x é y, y sumando despues, se obtiene esta otra: $m(x\eta - y\xi) = m$, y, por consecuencia, la determinante $x\eta - y\xi = +1$, de la sustitucion $\begin{pmatrix} x, & \xi \\ y, & \eta \end{pmatrix}$, por la cual se verifica realmente la trasformacion de la forma (a, b, c) en la (m, n, l). Se desprende asimismo de lo dicho que, por el contrario, cuando las dos formas (a, b, c) y (m, n, l) sean equivalentes, existirán siempre dos números (x, y) que verificarán las condiciones expresadas. De donde resulta que la existencia de los dos números (x, y) caracteriza por completo de equivalentes á las dos formas mencionadas.

c–) Ya poseemos los antecedentes necesarios para demostrar que el problema de *hallar todas las construcciones propias de un número dado* m, *por una forma dada* (a, b, c), se reduce á los dos fundamentales en la teoría de la equivalencia, al comenzar este capítulo expresados.

En efecto: el primero é indispensable requisito, segun consta en dichos antecedentes, para que una forma (a, b, c), con la determinante D, pueda representar un número m, es que tal determinante D, sea resto cuadrático de este número; pues, si esta condicion no se cumple, no existe ninguna construccion propia del número m por la forma (a, b, c). Admitamos, pues, que D es resto cuadrático de m, ó lo que es igual, que se verifica la congruencia (4), y determinemos todas sus raices incongruentes (109). Representando n una de estas raices, en cuyo caso $n^2 \equiv D \,(\text{mod. } m)$ ó bien $n^2 - D = m\,l$, será (m, n, l) una forma determinada, con la determinante D. Ahora bien, siempre que exista una

construccion (x, y), del número m por la forma (a, b, c), que *pertenezca* á la raiz n (representante de su clase), la forma (a, b, c) será equivalente á la (m, n, l); y dicha construccion (x, y) producirá entónces una sustitucion $\begin{pmatrix} x, & \xi \\ y, & \eta \end{pmatrix}$, por la cual se convertirá la primera forma en la segunda; pero una sola sustitucion, pues entre todas las soluciones de la ecuacion $x\eta - y\xi = +1$, determinante de aquélla, sólo existe una (η, ξ), que hace la expresion

$$(ax + by)\xi + (bx + cy)\eta$$

exactamente igual al individuo n. Luego para asegurar que existe, ó no, una construccion (x, y), del número m por la forma (a, b, c), perteneciente á la raiz individual n, de la congruencia (4), es preciso saber de antemano si las dos formas (a, b, c) y (m, n, l), que tienen igual determinante D, son, ó no son equivalentes: y este es el *primer* problema fundamental de las equivalencias.

Supongamos que las dos formas son equivalentes, y $\begin{pmatrix} x, & \xi \\ y, & \eta \end{pmatrix}$ una sustitucion por la cual se convierte la forma (a, b, c) en la (m, n, l); los coeficientes, primero y tercero, (x é y), de tal sustitucion, representan una construccion propia del número m por la forma (a, b, c), perteneciente á la raiz determinada n; y, como de cada una de estas construcciones (x, y) pertenecientes á la raiz n, sólo puede deducirse una sustitucion, correspondiendo siempre á construcciones diferentes sustituciones diferentes tambien, segun hemos visto, y viceversa, resulta que habremos hallado todas las construcciones propias del número m por la forma (a, b, c), pertenecientes á la raiz n, cuando hayamos determinado todas las sustituciones $\begin{pmatrix} x, & \xi \\ y, & \eta \end{pmatrix}$, mediante las cuales se convierte la forma (a, b, c) en la (m, n, l); y este es el *segundo* problema fundamental de las equivalencias.

CAPITULO III.

Del segundo problema fundamental de las equivalencias en general.

Probado ya que la teoría de las formas, ó de la construccion de los números, equivale esencialmente á los dos problemas fundamentales de las equivalencias, pasemos á resolver estos problemas.

El primero, *averiguar si dos formas de la misma determinante son, ó no son equivalentes,* exije procedimientos muy distintos para su resolucion, segun que la determinante comun de las formas sea positiva ó negativa; pero mediante ellos, y sea cualquiera el signo de la determinante, se obtiene siempre una *sustitucion,* por la cual se convierte una de las dos formas en la otra. Conociendo, pues, por la resolucion del *primer* problema, no sólo que dos formas son en realidad equivalentes, sino una sustitucion además por la cual se trasforman una en otra, el *segundo* se reducirá á *deducir de tal sustitucion todas las demas;* y, como para resolver este último no hay que tomar en cuenta el signo de la determinante por de pronto, le anteponemos al primero.

140.—*Primera reduccion del segundo problema.—Divisores de las formas y de las clases.*

El enunciado explícito del problema que vamos á resolver es el siguiente:

Dada una sustitucion L, *por la cual se convierte una forma* φ, *en otra equivalente* ψ, *hallar todas las sustituciones* S, *que produzcan el mismo efecto que la dada.*

Demos por conocidas *todas* las sustituciones T, por las que torna en sí misma la forma φ; esta forma se convertirá evidentemente en la otra ψ, mediante todas las sustituciones TL, compuestas sucesivamente de cada una de las sustituciones T, y de la L, que corresponden, por consecuencia, á las sustituciones S que buscamos. Veamos

ahora si componiendo, como hemos dicho, cada una de las sustituciones T con la dada L, se encuentran efectivamente *todas* las sustituciones S, y además una sola vez cada una de ellas. Para esto designemos por L' la sustitucion inversa de la L; mediante esta sustitucion inversa L', se convertirá á su vez (137-*a*) la segunda forma ψ en la primera φ; y, si componemos todas las sustituciones S con la inversa L', las resultantes SL' trasformarán la forma primera φ en sí misma, y corresponderán, por lo tanto, á las que por T designamos. Escribiendo la igualdad consiguiente $SL' = T$, y recordando que la sustitucion compuesta de las dos inversas es $LL' = \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}$ cuya determinante es 1, resultan estas otras: $SL'L = S = TL$: las cuales demuestran que por el método de composicion antes expresado se obtienen efectivamente las sustituciones S. Y que por dicho procedimiento se halla cada una de estas sustituciones S, una sola vez, se prueba sencillamente. En efecto, de la igualdad $TL = S$ se deduce la $T = SL'$, y, por consecuencia, que la sustitucion T, por la cual se obtiene una sustitucion S, determinada, es tambien completamente determinada; es decir: que á sustituciones T, diferentes, corresponden sustituciones S, tambien diferentes: luego, del modo ya repetido, cada una de las sustituciones S, se obtendrá una sola vez.

Ahora bien, sabido que coincide el conjunto de todas las sustituciones S, que buscamos, con el de todas las sustituciones TL, compuestas de la conocida L, y de las T, aún desconocidas, sólo necesitaremos buscar estas T, para encontrar aquellas S; y así el problema en un principio enunciado queda reducido al siguiente:

Encontrar todas las sustituciones por las cuales una forma torna en sí misma.

Antes de proseguir conviene, para no interrumpir más tarde nuestros razonamientos, establecer en este punto algunas definiciones indispensables.

Sea σ el máximo comun divisor (positivo) de los tres números $a, 2b, c$; es claro que todos los números representados por la forma (a, b, c) serán múltiplos de σ: por lo cual llamaremos á este número σ, siempre que no pueda surgir duda ninguna, *el divisor de la forma* (a, b, c). Con relacion á este *divisor*, debemos considerar dos casos:

1.° *Que el cociente* $2b : \sigma$ *sea par*. Entónces el divisor σ debe estar

contenido en b, y su cuadrado σ^2, por consecuencia, en la determinante $D = b^2 - ac$. Y recíprocamente: cuando la determinante D sea divisible por el cuadrado σ^2, ó se verifique la congruencia $D \equiv 0 \pmod{\sigma^2}$, el coeficiente b será tambien divisible por σ; el cociente $2b : \sigma$ par; y el divisor σ será al mismo tiempo el máximo comun divisor de los números a, b, c.

2.° *Que el cociente* $2b : \sigma$ *sea impar.* Para esto es necesario que σ sea siempre par; el cuadrado σ^2 no estará entónces contenido en D, pero sí en $4D = (2b)^2 - 4ac$, siendo

$$\frac{4D}{\sigma^2} = \left(\frac{2b}{\sigma}\right)^2 - 4\frac{ac}{\sigma\sigma} \equiv 1 \pmod{4};$$

y, por lo tanto: $4D \equiv \sigma^2 \pmod{4\sigma^2}$. Y, recíprocamente: si se verifica la congruencia $4D \equiv \sigma^2 \pmod{4\sigma^2}$, se realizará tambien esta otra $(2b)^2 \equiv \sigma^2 \pmod{4\sigma^2}$: el cociente $2b : \sigma$, por consecuencia, será impar; y $\frac{1}{2}\sigma$ el máximo comun divisor de los números a, b, c.

De lo dicho se desprende que el divisor σ, de toda forma cuya determinante sea D, ha de satisfacer necesariamente á una de las dos congruencias:

$$D \equiv 0 \pmod{\sigma^2} \quad \text{ó} \quad 4D \equiv \sigma^2 \pmod{4\sigma^2}.$$

Y, recíprocamente: siempre que un número positivo σ, verifique alguna de estas dos congruencias, existirá una forma (a, b, c), de determinante D, cuyo divisor será dicho número σ. Así, segun que σ satisfaga á la primera ó á la segunda condicion, la forma

$$\left(\sigma, 0, \frac{-D}{\sigma}\right), \text{ ó la } \left(\sigma, \tfrac{1}{2}\sigma, \frac{\sigma^2 - 4D}{4\sigma}\right),$$

tendrán por determinante D, y por divisor σ. Cada una de estas dos

formas se denomina *simple* (*simplicissima*), y la simple $(1, 0, -D)$, cuyo divisor es la unidad, *principal*.

Tambien hemos visto en los dos casos estudiados que el máximo comun divisor τ, de los tres números a, b, c, es en el primero σ, y en el segundo $\frac{1}{2}\sigma$. Si $\tau = 1$, y entónces los tres números a, b, c, son primos relativos, la forma (a, b, c) se llama *primitiva;* y, si $\tau > 1$, y establecemos las igualdades $a = \tau a'$, $b = \tau b'$, $c = \tau c'$, $b'b' - a'c' = D'$, $D = \tau^2 D'$, la forma (a, b, c) se llamará *derivada* de la forma primitiva (a', b', c') de determinante D'. Pero en las formas primitivas hay que distinguir dos especies: si en la forma primitiva (a, b, c), no son pares al mismo tiempo los coeficientes a, c, no sólo los números a, b, c sino además los $a, 2b, c$ serán primos entre sí, en cuyo caso tambien $\sigma = 1$, y la expresada forma (a, b, c) se denominará *propiamente primitiva*, *forma propia*, ó de *primera especie;* y, si los coeficientes a, c son al mismo tiempo pares, y $\sigma = 2$, la forma primitiva (a, b, c), se denominará *impropiamente primitiva*, *forma impropia*, ó de *segunda especie*. En este último caso tiene que ser b necesariamente impar; puesto que de otro modo no sería primitiva la forma (a, b, c); y, como entónces $b^2 \equiv 1 \pmod 4$, y, además ac es divisible por 4, será la determinante $b^2 - ac = D \equiv 1 \pmod 4$: es decir, que las formas primitivas de segunda especie tienen su determinante de la forma $4n + 1$, cuando es positiva, ó de la forma $-(4n + 3)$, cuando sea negativa. Todo lo cual se deduce de las consideraciones que al principio expusimos.

Por otra parte, de las fórmulas de trasformacion (135) se desprende que, cuando una forma (a', b', c') se halla contenida en otra (a, b, c), todo divisor comun de los números $a, 2b, c$, lo será asimismo de los $a', 2b', c'$: luego dos formas equivalentes tendrán el mismo divisor σ, el cual será, por consecuencia, comun á todas las formas pertenecientes á una misma clase, y se llamará *divisor de la clase*. Lo mismo acontece con el máximo comun divisor τ de los números a, b, c respecto de todas las formas (a, b, c), que á la misma clase correspondan. Así que cuando en una clase figure una forma *simple*, *de divisor* σ, ó una forma *principal*, ó una *primitiva*, de cualquier especie, ó una *derivada*, todas las formas comprendidas en ella serán respectivamente homogéneas con cada una de las enumeradas; y dicha clase llevará tambien los nombres

correspondientes de *simple, principal, primitiva,* de *primera* ó *segunda especie,* y *derivada.*

Por último, así como todas las formas de igual determinante D, y con el mismo divisor σ, constituyen un *órden*, lo constituye tambien el conjunto de todas las clases que tengan la determinante D, y el divisor σ. En consecuencia, y para ser más explícitos, dos clases, cuyos representantes sean las formas (a, b, c) y (a', b', c'), pertenecerán al *mismo órden*, si, no sólo los números a, b, c y a', b', c', tienen el mismo máximo comun divisor, sino tambien los números $a, 2b, c$ y los $a', 2b', c'$; y pertenecerán á *diversos órdenes*, cuando una de estas dos condiciones, ó las dos, no tengan cumplimiento. De lo cual se infiere inmediatamente que las formas primitivas de la primera especie constituirán un solo órden; las primitivas de segunda especie, otro; etc.

141.—*Segunda reduccion del segundo problema.—Ecuacion de Pell.*

El problema que estamos estudiando, reducido ya en el artículo precedente á *encontrar todas las sustituciones por las cuales una forma se convierte en sí misma,* todavía puede recibir otra simplificacion.

Admitamos que $\begin{pmatrix} \lambda, & \mu \\ \nu, & \rho \end{pmatrix}$ sea una sustitucion por la cual torna en sí misma la forma (a, b, c), de determinante D, y divisor σ. Desde luego se verificará la ecuacion

$$\lambda\rho - \mu\nu = 1 \qquad (1)$$

y además (135) estas otras:

$$a\lambda^2 + 2b\lambda\nu + c\nu^2 = a \qquad (2)$$

$$a\lambda\mu + b(\lambda\rho + \mu\nu) + c\nu\rho = b \qquad (3).$$

De las tres se infiere por de pronto que la forma (a, b, c), por la

sustitucion $\begin{pmatrix} \lambda, & \mu \\ \nu, & \rho \end{pmatrix}$ se convierte en otra equivalente, cuyos coeficientes, primero y tercero, son a y b; y el tercero c', de esta nueva forma, es tambien igual al tercero de la propuesta c, á causa de ser iguales las determinantes de ambas: de lo cual resulta que la sustitucion admitida se halla completamente caracterizada por las tres ecuaciones anteriores.

No podria asegurarse lo mismo si, en lugar de la primera de ellas, tomáramos la relativa al tercer coeficiente,

$$a\mu^2 + 2b\mu\rho + c\rho^2 = c;$$

pues de aquí, retrocediendo, no se deduce exclusivamente el único valor de la determinante de la sustitucion establecida, necesario para que ésta sea propia, sino el ambíguo $\lambda\rho - \mu\nu = \pm 1$.

Si las ecuaciones (1), (2), (3) caracterizan y determinan la sustitucion $\begin{pmatrix} \lambda, & \mu \\ \nu, & \rho \end{pmatrix}$, veamos cómo se hallan estos coeficientes λ, μ, ν, ρ, mediante aquellas ecuaciones. Para esto sustitúyase en la (3) por $\lambda\rho$ su valor $\mu\nu + 1$, deducido de la (1); y, eliminando entre la ecuacion así resultante

$$a\lambda\mu + 2b\mu\nu + c\nu\rho = 0 \qquad (3')$$

y la (2), primeramente $2b$, y luégo c, se obtendrán las siguientes:

$$a\mu + c\nu = 0, \quad \text{y} \quad a(\lambda - \rho) + 2b\nu = 0.$$

Estas ecuaciones, como a no puede ser cero, quedan satisfechas evidentemente por los tres valores:

$$\nu = \frac{a}{\sigma}u, \quad \mu = -\frac{c}{\sigma}u, \quad \text{y} \quad (\lambda - \rho) = -\frac{2b}{\sigma}u \qquad (4)$$

en los cuales figura una nueva incógnita u, que significará siempre un número *entero;* por ser enteros los coeficientes de sustitucion $\nu, \mu, \lambda\rho$, y σ el máximo comun divisor de $a, c, 2b$.

Poniendo en la ecuacion (1) los valores de ν y μ, se obtiene esta otra:

$$\lambda\rho = -\frac{ac}{\sigma^2}u^2 + 1:$$

de la cual, teniendo en cuenta la igualdad evidente

$$(\lambda+\rho)^2 = (\lambda-\rho)^2 + 4\lambda\rho,$$

y el valor para $\lambda - \rho$ antes escrito (4), resulta:

$$(\lambda+\rho)^2 = (\lambda-\rho)^2 + 4\lambda\rho = \frac{4b^2}{\sigma^2}u^2 - \frac{4ac}{\sigma^2}u^2 + 4 = \frac{4(Du^2+\sigma^2)}{\sigma^2}$$

ó bien:

$$\left(\frac{\sigma(\lambda+\rho)}{2}\right)^2 = Du^2 + \sigma^2.$$

Y esta última igualdad demuestra que $\frac{1}{2}\sigma(\lambda+\rho)$ debe ser siempre un número *entero*. Designémosle por t, y resultará que:

$$\lambda + \rho = \frac{2t}{\sigma} \quad \text{y} \quad t^2 = Du^2 + \sigma^2. \tag{5}$$

En atencion á las ecuaciones (4) y (5), podemos resumir lo antedicho como sigue:

Si $\begin{pmatrix}\lambda, & \mu\\ \nu, & \rho\end{pmatrix}$ *expresa una sustitucion por la cual se convierte en sí misma la forma* (a, b, c), *de determinante* D y *divisor* σ, *los valores de los cuatro coeficientes de tal sustitucion son los siguientes:*

$$\begin{aligned} \lambda &= \frac{t - bu}{\sigma}, & \mu &= -\frac{cu}{\sigma} \\ \nu &= \frac{au}{\sigma}, & \rho &= \frac{t + bu}{\sigma}. \end{aligned} \tag{I}$$

en los cuales designan t *y* u *dos números enteros, por determinar, que deben verificar la ecuacion*

$$t^2 - D u^2 = \sigma^2. \qquad \text{(II)}$$

Nos resta probar todavía, y es de gran interés, que la recíproca de esta proposicion es cierta; ó que:

Siendo t, u *dos números enteros que verifican la ecuacion* (II), *por las ecuaciones* (I) *se determinan los cuatro coeficientes enteros* λ, μ, ν, ρ, *de una sustitucion* $\begin{pmatrix} \lambda, & u \\ \nu, & \rho \end{pmatrix}$, *por la cual se convierte en sí misma la forma* (a, b, c).

Para esto demostraremos primeramente que los números λ, μ, ν, ρ, son enteros. Desde luego lo son evidentemente cuando $\sigma = 1$; pero supongamos que σ no tenga este valor particular. Entónces, como a y c son divisibles por σ, los números μ y ν son enteros, segun sus fórmulas lo manifiestan. Por otra parte σ^2 está contenido en $4D$, y, á causa de la igualdad $4t^2 - 4Du^2 = 4\sigma^2$, tambien deberá ser $4t^2$ divisible por σ^2, y, por consecuencia, $2t$ divisible por σ; y, como σ está contenido además en $2b$, resulta (I) que 2λ y 2ρ serán números enteros cuya suma $4t : \sigma$ es par: lo cual exige que dichos sumandos 2λ y 2ρ sean los dos pares, ó los dos impares. Mas el producto de estos mismos números,

$$2\lambda \times 2\rho = 4\,\frac{t^2 - b^2 u^2}{\sigma^2} = 4\,\frac{\sigma^2 - a c u^2}{\sigma^2} = 4\left(1 - \frac{a c}{\sigma\sigma}\, u^2\right),$$

es evidentemente par: luego 2λ y 2ρ serán pares, y para esto es necesario que λ y ρ sean enteros.

Demostrado que los números μ, ν, λ, ρ, son enteros, basta sustituir sus valores (I), teniendo presente la ecuacion (II), en las (1), (2) y (3) para ver que éstas quedan por tales valores satisfechas; y esto prueba que la forma (a, b, c) por la sustitucion $\begin{pmatrix} \lambda, & \mu \\ \nu, & \rho \end{pmatrix}$ torna en sí misma.

Conclúyese de cuanto precede que, de una sustitúcion conocida $\begin{pmatrix}\lambda, & \mu\\ \nu, & \rho\end{pmatrix}$, puede siempre deducirse una solucion t, u, de la ecuacion (II), mediante las fórmulas (I); y recíprocamente. Mas estas fórmulas son de tal naturaleza que á cada par de valores dados (t, u), corresponde un solo sistema de valores para los números λ, μ, ν, ρ; y recíprocamente: á cada sistema de valores dados para λ, μ, ν, ρ, corresponde uno solo para t, u. De donde se infiere que á sustituciones diferentes $\begin{pmatrix}\lambda, & \mu\\ \nu, & \rho\end{pmatrix}$, corresponden tambien soluciones diferentes (t, u), de la ecuacion (II): con lo cual el problema enunciado en un principio se reduce por último á

Determinar todas las soluciones enteras de la ecuacion $t^2 - Du^2 = \sigma^2$.

Esta ecuacion lleva el nombre del matemático inglés *Pell* que la resolvió, aunque no de un modo general y completo, antes que ninguno.

142.—*Resolucion de la ecuacion de Pell para las determinantes negativas.—Conclusion del segundo problema para estas determinantes.*

Designemos de una vez para siempre por Δ el valor absoluto de la determinante D: entónces, siendo ésta negativa, $D = -\Delta$; y la ecuacion (II) correspondiente,

$$t^2 + \Delta u^2 = \sigma^2$$

tendrá un número *finito* de soluciones (t, u). Para hallarlas distinguiremos dos casos (140):

1.° $D \equiv 0 \pmod{\sigma^2}$; y, de consiguiente, Δ divisible por σ^2. Aquí debemos considerar que Δ puede ser divisible por σ^2, siendo mayor ó igual á este divisor. Si ocurre lo primero, esto es, $\Delta > \sigma^2$, la ecuacion (II) tendrá 2 soluciones, á saber:

$$t = +\sigma \qquad t = -\sigma$$

$$u = 0 \qquad u = 0;$$

si lo segundo, $\Delta = \sigma^2$, la ecuacion (II) tendrá 4 soluciones:

$$t = +\sigma \qquad t = -\sigma \qquad t = 0 \qquad t = 0$$
$$u = 0 \qquad u = 0 \qquad u = 1 \qquad u = -1$$

2.° $4D \equiv \sigma^2 \pmod{4\sigma^2}$, y, por consecuencia, $4\Delta \equiv 3\sigma^2 \pmod{4\sigma^2}$. Esta última congruencia puede verificarse de dos modos principales: siendo $4\Delta > 3\sigma^2$ y, por tanto, $4\Delta \geqq 7\sigma^2$; ó bien $4\Delta = 3\sigma^2$. En el supuesto $4\Delta > 3\sigma^2$, la ecuacion (II) admite siempre 2 soluciones:

$$t = \sigma \qquad t = -\sigma$$
$$u = 0 \qquad u = 0;$$

y en el de ser $4\Delta = 3\sigma^2$, admite las 6 siguientes:

$$t = +\sigma, \quad t = +\tfrac{1}{2}\sigma, \quad t = +\tfrac{1}{2}\sigma, \quad t = -\sigma, \quad t = -\tfrac{1}{2}\sigma, \quad t = -\tfrac{1}{2}\sigma$$
$$u = 0, \quad u = +1, \quad u = -1, \quad u = 0, \quad u = -1, \quad u = +1$$

Aplicando estos principios generales á las formas primitivas, llamadas por Dirichlet de primera y segunda especie (140), fácilmente encontraríamos las soluciones de las ecuaciones (II) correspondientes, y por las fórmulas (I) las sustituciones $\begin{pmatrix} \lambda, & \mu \\ \nu, & \rho \end{pmatrix}$. Así, por ejemplo: para las formas primitivas de la primera especie, cuyo divisor es $\sigma = 1$, la ecuacion correspondiente

$$t^2 + \Delta u^2 = 1,$$

en la hipótesis de ser $\Delta > 1$, tendrá las 2 soluciones opuestas:

$$t = +1 \qquad t = -1$$
$$u = 0 \qquad u = 0$$

de las cuales se deducen (I) las 2 únicas sustituciones:

$$\begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} -1, & 0 \\ 0, & -1 \end{pmatrix};$$

y, en el supuesto de ser $\Delta = 1$, dicha ecuacion admitirá las 4 soluciones:

$$\begin{array}{cccc} t = +1 & t = -1 & t = 0 & t = 0 \\ u = 0 & u = 0 & u = +1 & u = -1, \end{array}$$

que producen las 4 sustituciones:

$$\begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}, \quad \begin{pmatrix} -1, & 0 \\ 0, & -1 \end{pmatrix}, \quad \begin{pmatrix} -b, & -c \\ +a, & +b \end{pmatrix}, \quad \begin{pmatrix} +b, & +c \\ -a, & -b \end{pmatrix},$$

mediante las cuales torna en sí misma la forma primitiva, de la primera especie, (a, b, c), cuya determinante es $b^2 - ac = -1$.

Y análogas consideraciones pudiéramos hacer respecto de las formas primitivas de la segunda especie, para las cuales toma la ecuacion de Pell la forma

$$t^2 + \Delta u^2 = 4.$$

En conclusion: si con la sencillez que hemos procedido, tratándose de las determinantes *negativas*, supiéramos tambien resolver la ecuacion de *Pell* para las determinantes *positivas*, el segundo problema fundamental de las equivalencias, estaria completamente terminado; pero la resolucion de la ecuacion mencionada, referida á las determinantes positivas, léjos de ser fácil, presenta dificultades que no pueden orillarse del todo en este momento; sino despues de haber estudiado el primer problema de las equivalencias (139) que, como sucede con la ecuacion de Pell, es mucho ménos complicado para las formas de determinante negativa que para las de determinante positiva. Por estas razones dejamos en suspenso por ahora el segundo problema, en cuanto se refiere á las determinantes positivas, para concluirlo en su lugar oportuno, y pasamos á estudiar el primero, respecto de unas y otras determinantes, como se verá en los capítulos siguientes.

CAPITULO IV.

Del primer problema fundamental de las equivalencias para las determinantes negativas.

143.—*Limitaciones en este problema.—Formas reducidas.*

El primer problema fundamental en la teoría de las equivalencias, ya anteriormente enunciado (139) es éste:

Averiguar si dos formas dadas, con iguales determinantes, son ó no son equivalentes.

Así expresado en general comprende, tanto las formas de determinante negativa, como las de determinante positiva; pero ya en el epígrafe del capítulo se establece una limitacion, concretándole á las de determinante negativa; y todavía de esta limitacion se desprenden otras para estas formas, que debemos fijar previamente.

Desde luego, siendo $D = -\Delta$, como ya quedó sentado (142), los coeficientes extremos a y c, de la forma de determinante negativa,

$$\varphi = a x^2 + 2 b x y + c y^2,$$

deben tener por necesidad el mismo signo; pues $ac = b^2 + \Delta$ es siempre positivo; y, como ademas

$$a \varphi = (a x + b y)^2 + \Delta y^2,$$

todos los números representados por la forma φ habrán de tener necesariamente el mismo signo que a y c. Si, pues, las dos formas (a, b, c) y (a', b', c') son equivalentes, los coeficientes extremos a', c', de la última llevarán el mismo signo que los de la primera; y, como de la

equivalencia de dichas dos formas se desprende tambien la de estas otras $(-a, -b, -c)$ y $(-a', -b', -c')$, podremos concretarnos en adelante á las formas llamadas *positivas,* esto es, á aquellas cuyos coeficientes extremos sean *positivos.*

Mas con todas estas limitaciones no podemos decidir todavía si dos formas de esta especie son, ó no, equivalentes de un modo directo; sino valiéndonos, como intermediarias, de otras, aún más particulares dentro de aquéllas, que llevan el nombre de *reducidas.* Se dirá que una forma (A, B, C), de determinante negativa, y coeficientes extremos positivos, es *reducida*, cuando sus coeficientes satisfagan á las condiciones:

$$C \geqq A \geqq 2\,(B)$$

designando por (B) el valor absoluto del coeficiente medio B: las cuales en lenguaje vulgar expresan que el último coeficiente no sea menor que el primero, ni éste tampoco menor que el duplo (en valor absoluto) del coeficiente medio.

Escribiendo las anteriores condiciones de este otro modo:

$$2\,(B) \leqq A, \quad A \leqq C,$$

se deducen con facilidad otras particulares que tienen importancia para lo sucesivo, á saber:

$$(B) \leqq \sqrt{\tfrac{1}{3}\,\Delta}, \text{ y especialmente } A \leqq \sqrt{\tfrac{4}{3}\,\Delta}.$$

Para obtenerlas, el camino es el siguiente: de las relaciones que definen la forma reducida (A, B, C) se desprenden evidentemente: $4B^2 \leqq A^2$, $A^2 \leqq AC$, y por consecuencia: $4B^2 \leqq AC$ ó $3B^2 \leqq AC - B^2 = \Delta$, de la cual resulta: $(B) \leqq \sqrt{\tfrac{1}{3}\Delta}$. Como, por otra parte, $AC = \Delta + B^2$, y asimismo $3AC = 3\Delta + 3B^2$, y $3B^2 \leqq \Delta$, será $3AC \leqq 4\Delta$; y con mayor razon, por ser $A^2 \leqq AC$, se verificará la condicion $3A^2 \leqq 4\Delta$, ó bien la escrita arriba: $A \leqq \sqrt{\tfrac{4}{3}\,\Delta}$.

144. — *Equivalencia entre una forma cualquiera, de determinante negativa, y otra forma reducida.*

Veamos ahora si, dada una forma cualquiera, de determinante negativa, podemos hallar siempre otra forma equivalente á ella, pero que sea *reducida*. Para esto, como sabemos ya que las formas *contíguas* son equivalentes (137-*a*), bastará considerar las formas contíguas de la propuesta, y ver si entre ellas existe alguna que sea, en efecto, reducida.

Sea, pues, la forma dada (a, b, a'): entre sus contíguas por la derecha (a', b', a''), existirá siempre una (y á veces dos) en la cual se verificará la condicion $a' \geqq 2(b')$, exigida antes para las reducidas; porque entre todos los números congruentes con $-b$, segun el módulo a', existe uno, b', cuyo valor absoluto (b'), tomando el mínimo, será seguramente menor, ó igual á lo sumo á $\frac{1}{2}a'$; (sólo en el caso de ser par a', y $b \equiv \frac{1}{2}a'$ (mod. a'), existirian dos números, ó valores de b', á saber: $\pm\frac{1}{2}a'$). Luego no hay inconveniente en establecer como ciertas la congruencia $b' \equiv -b$ (mod. a'), y la relacion $2(b') \leqq a'$; y, determinado por ellas el valor de b', la igualdad $b + b' = -a'\delta$ nos dará el de δ, y, por consecuencia, nos será conocida la sustitucion

$$\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$$

mediante la cual se convierte la forma dada (a, b, a') en su contígua por la derecha (a', b', a''). Para esta última se cumple, como hemos dicho, una de las condiciones, á saber, $2(b') \leqq a'$, que definen las formas reducidas; de modo que, si tambien se verificase la otra condicion, $a' \leqq a''$, aquella forma, (a', b', a''), sería reducida, y además la que buscábamos.

Pero supongamos que así no suceda, sino que, por el contrario, en

vez de la condicion $a' \leqq a''$, se verifique la opuesta $a' > a''$: entónces aplicaremos á la forma (a', b', a'') el mismo procedimiento que á la propuesta (a, b, a'): esto es, hallaremos la forma (a'', b'', a'''), contígua de la (a', b', a'') por la derecha, en la cual se verificará de seguro, como ya sabemos, la condicion $2(b'') \leqq a''$, y veremos si tambien se cumple la otra $a'' \leqq a'''$; en cuyo caso nuestra operacion estaria terminada. Mas, si tampoco en la forma (a'', b'', a''') se cumpliese la condicion última, $a'' \leqq a'''$, para ser reducida, la aplicaríamos el mismo procedimiento que á las dos anteriores, y así continuaremos hasta encontrar una forma, contígua de la anterior por la derecha, que sea reducida. La cuestion ahora está en saber si tendrá fin el número de operaciones necesarias, segun el procedimiento explicado, para determinar esta forma reducida; mas no es difícil desvanecer esta duda. En efecto, para que ninguna de las formas contíguas, que por el método explicado se van encontrando sucesivamente, fuese reducida, sería necesario que no tuviese fin la série de los números enteros

$$a', a'', a''', \ldots\ldots a^{(n)}, a^{(n+1)}$$

cada uno de los cuales es menor que el anterior en una unidad por la parte más corta; y, como esto no es posible, pues siempre es finito el número de enteros positivos, menores que uno dado, resulta que por precision habremos de encontrar, del modo que se ha dicho, una forma última $(a^{(n)}, b^{(n)}, a^{(n+1)})$, en la cual no sólo tendrá lugar la condicion siempre cumplida, $2(b^{(n)}) \leqq a^{(n)}$, sino tambien la contingente $a^{(n)} \leqq a^{(n+1)}$, que será, por consecuencia, reducida. Y no solamente hallamos esto; mediante las mismas operaciones que practicamos se encuentra además una sustitucion, compuesta de todas las intermedias de la forma $\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$, que convierte realmente la forma dada (a, b, a') en su equivalente reducida $(a^{(n)}, b^{(n)}, a^{(n+1)})$.

Para mayor claridad resolveremos un ejemplo. Sea la forma dada (200, 100, 51) cuya determinante es $D = -200$. Por la congruencia $b' \equiv -100 \pmod{51}$, determinamos el valor de $b' = 2$; y por la igualdad consiguiente, $b + b' = 102 = -51\,\delta$, el valor de $\delta = -2$;

y ya tenemos la sustitucion $\begin{pmatrix} 0, & 1 \\ -1, & -2 \end{pmatrix}$ por la que se convertirá la forma dada en su contígua por la derecha. Mas no hace falta valerse de tal sustitucion para encontrar esta forma contígua; pues, conocidos sus dos primeros coeficientes a', b', y su determinante D, su tercer coeficiente a'', puede calcularse fácilmente por la fórmula

$$a'' = \frac{b'^2 - D}{a'},$$

que, aplicada al ejemplo propuesto, da:

$$a'' = \frac{4 + 200}{51} = 4.$$

Así, la forma contígua por la derecha de la dada es $(51, 2, 4)$. Pero en esta última no se verifica la condicion $a' \leqq a''$, ó $51 \leqq 4$. Aplicando, pues, á la forma hallada $(51, 2, 4)$, el mismo procedimiento que á la primitiva, tendremos: $b'' \equiv -2 \pmod 4$: de donde $b'' = \pm 2$; y, por consecuencia, las dos sustituciones, segun se tome el signo superior ó el inferior en el doble valor de b'', $\begin{pmatrix} 0, & 1 \\ -1, & -1 \end{pmatrix}$ ó $\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}$. Además, como antes,

$$a''' = \frac{4 + 200}{4} = 51;$$

y, unido este tercer coeficiente 51, con los dos, $a'' = 4$, $b'' = \pm 2$, ya conocidos, se obtiene la doble forma $(4, \pm 2, 51)$ que es ya reducida.

Resulta, finalmente, que la forma propuesta $(200, 100, 51)$, por la sustitucion compuesta (136)

$$\begin{pmatrix} 0, & 1 \\ -1, & -2 \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & -1 \end{pmatrix} = \begin{pmatrix} -1, & -1 \\ 2, & 1 \end{pmatrix},$$

se convierte en la forma (4, 2, 51); y, por la otra sustitucion

$$\begin{pmatrix} 0, & 1 \\ -1, & -2 \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} = \begin{pmatrix} -1, & 0 \\ 2, & -1 \end{pmatrix},$$

en la otra forma (4, —2, 51).

145.—*Equivalencia entre dos formas reducidas.*

Del ejemplo que acabamos de resolver se desprende que dos formas reducidas, distintas, pueden ser equivalentes á una misma forma; y, por consecuencia, que aquellas dos formas reducidas pertenecen á la misma clase, esto es, son tambien equivalentes entre sí.

Es de grande interés averiguar en general:

Cuándo dos formas reducidas (a, b, c) *y* (a', b', c'), *con igual determinante negativa* $D = -\Delta$, *serán entre sí equivalentes.*

Demos por cierto que las dos formas (a, b, c) y (a', b', c') son equivalentes; y establezcamos ademas la condicion

$$a' \leqq a,$$

que en nada coarta la generalidad del asunto.

Si $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ es una sustitucion propia que trasforma la (a, b, c) en la (a', b', c'), se verificarán las ecuaciones (135):

$$1 = \alpha\delta - \beta\gamma \qquad (1)$$

$$a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \qquad (2)$$

$$b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta \qquad (3)$$

y, además, multiplicando por a la segunda, esta otra:

$$aa' = (a\alpha + b\gamma)^2 + \Delta\gamma^2 \qquad (4).$$

Ahora bien, por ser reducidas las dos formas propuestas, se verificarán las condiciones:

$$a \leqq \sqrt{4/3\,\Delta}, \quad a' \leqq \sqrt{4/3\,\Delta};\ \text{y, por lo tanto: } aa' \leqq 4/3\,\Delta.$$

La última exige esta otra: $\gamma^2 = 0$ ó $\gamma^2 = 1$; porque, si fuese $\gamma^2 \geqq 4$, de la ecuacion (4) resultaria $aa' \geqq 4\Delta$: en oposicion con aquélla. Estudiemos con separacion cada uno de losdos casos indicados.

1.° $\gamma = 0$.

Con esta suposicion las tres ecuaciones (1), (2) y (3) se trasforman en las siguientes:

$$1 = \alpha\delta: \qquad a' = a\alpha^2; \qquad b' = a\alpha\beta + b.$$

De la primera resulta: $\alpha = \delta = \pm 1$; la segunda, por lo tanto, se convierte en la $a' = a$, y la tercera en esta otra: $b' - b = \pm a\beta$: la cual expresa que la diferencia $b' - b$ es divisible por $a = a'$. Mas esta division, como $(b) \leqq \frac{1}{2}a$, $(b') \leqq \frac{1}{2}a'$, y de consiguiente, $(b') \leqq \frac{1}{2}a$, sólo es posible de dos modos: ó siendo $b' - b = 0$, y entónces $b' = b$, y tambien, por ser ya $a' = a$, será $c' = c$; en cuyo caso las dos formas serán idénticas: ó siendo $b' - b = a$, en valor absoluto; puesto que no puede ser $b' - b > a$; y entónces uno de los números b ó b' tiene que ser igual á $\frac{1}{2}a$, y el otro igual á $-\frac{1}{2}a$. Y, en este caso, como tambien es $c' = c$, las dos formas propuestas se convertirán en las ambíguas (*ancipites*) no idénticas, pero en realidad equivalentes, $(a, \frac{1}{2}a, c)$ y $(a, -\frac{1}{2}a, c)$; trasformándose la primera en la segunda por la sustitucion $\begin{pmatrix} 1, -1 \\ 0, +1 \end{pmatrix}$.

2.° $\gamma = \pm 1$.

En esta hipótesis, la ecuacion (2) se reduce á la siguiente:

$$a' = a\alpha^2 \pm 2b\alpha + c;$$

de la cual, como al principio sentamos que a' no era mayor que a, y por consecuencia, tampoco mayor que c, se desprende la condicion:

$$a\alpha^2 \pm 2b\alpha \leqq 0.$$

Mas, por otra parte, como $2(b) \leqq a$, y evidentemente $(\alpha) \leqq \alpha^2$, lo cual prueba que el valor absoluto de $2b\alpha$ no es mayor que $a\alpha^2$, tenemos tambien:

$$a\alpha^2 \pm 2b\alpha \geqq 0.$$

Y de las dos se deduce que, no pudiendo ser positivo ni negativo su primer miembro comun, por precision:

$$a\alpha^2 \pm 2b\alpha = 0,$$

y, por lo tanto, $a' = c$: igualdad que exige además, por haber establecido las relaciones $a' \leqq a$ y $a \leqq c$, que se verifiquen éstas otras: $a' = a$ y $c = a$. Teniéndolas presentes, y con ellas la $2b\alpha = \mp a\alpha^2$, la ecuacion (3), con auxilio de la (1), toma la forma:

$$b + b' = a(\alpha\beta \mp \alpha^2\delta \pm \delta),$$

y expresa ser $b + b'$ divisible por a. De esta circunstancia se colije fácilmente, como antes hicimos, que la suma $b + b'$, ó es igual á *cero*, ó su valor absoluto igual al de a. Si sucede esto último, b y b' serán iguales entre sí y cada uno de ellos valdrá $+\frac{1}{2}a$ ó $-\frac{1}{2}a$; y entónces nos hallamos con dos formas idénticas, cuya equivalencia es evidente, y que no ofrecen ningun interés. Pero, si acontece lo primero, esto es, $b + b' = 0$, ó $b' = -b$, y, por consecuencia, $a' = a$ y $c = a$,

tendremos, por el contrario, dos formas (a, b, a) y $(a, -b, a)$, que (cuando no sea $b = 0$) no serán idénticas, aunque sí equivalentes; convirtiéndose la primera en la segunda por la sustitucion $\begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix}$. Resumiendo todo lo dicho:

Las dos formas $(a, \frac{1}{2}a, c)$ y (a, b, a), *que se convierten respectivamente, por las sustituciones,*

$$\begin{pmatrix} 1, & -1 \\ 0, & +1 \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix},$$

en las $(a, -\frac{1}{2}a, c)$ y $(a, -b, a)$, *representan los dos únicos casos en que dos formas reducidas, no idénticas, son equivalentes.*

Es decir, que las formas (a, b, c) y (a', b', c'') no podrán ser equivalentes si no fueren *opuestas*, y ademas *ambiguas*, ó con sus coeficientes extremos iguales. Mas, como la equivalencia de que aquí se habla es la *propia*, y las formas opuestas son (137-*a*) *impropiamente* equivalentes, parece que existe contradiccion entre las dos afirmaciones.

Deteniéndose un poco, sin embargo, á examinar las formas reducidas, presentadas en la conclusion anterior, como equivalentes en el sentido propio, desaparece semejante duda. Las formas opuestas (a, b, c) y $(a, -b, c)$, sin decir más, son, en efecto, impropiamente equivalentes; pero, si en ellas se verifica la condicion $a = c$, serán además contíguas, y por lo tanto propiamente equivalentes; y, si se verifica la $2b = a$, la forma entónces *anceps* (a, b, c), será propiamente equivalente á la $(c, -b, a)$, la cual es contígua de la $(a, -b, c)$; y, como las formas contíguas son propiamente equivalentes, del mismo modo lo será la $(c, -b, a)$ con las (a, b, c) y $(a, -b, c)$; y, por consecuencia, estas dos últimas entre sí.

Para saber ahora tambien cuándo dos formas reducidas (a, b, c) y (a', b', c'), no opuestas, serán impropiamente equivalentes, basta considerar que así sucederá siempre que las no idénticas (a, b, c) y $(a', -b', c')$ lo sean propiamente, y al contrario. De donde resulta que, para ser aquéllas impropiamente equivalentes, es necesario que sean idénticas y

además ancípites, ó que se verifique en ellas la condicion $a = c$; y, por consecuencia, que dos formas reducidas que no sean idénticas ni opuestas, tampoco podrán ser propia, ni impropiamente equivalentes.

146.—*Resúmen.*

El problema cuyo objeto es averiguar si dos formas de igual determinante negativa son, ó no, equivalentes, está completamente resuelto con el auxilio de las formas reducidas; mas todavía requiere este asunto algunas explicaciones que compendien y esclarezcan la doctrina referente al mismo, expuesta en los artículos que anteceden.

Designemos por φ y ψ las dos formas cuya equivalencia se trata de averiguar: si no fuesen ya reducidas, se trasformará cada una de ellas, como sabemos, en otra reducida equivalente, esto es, φ en φ' y ψ en ψ'; y, si estas formas φ' y ψ' fuesen idénticas, ó estuviesen comprendidas en alguno de los dos casos de excepcion antes marcados, lo cual se conoce á simple vista, las propuestas φ y ψ serian equivalentes.

Nótese tambien que, por el procedimiento de reduccion explicado, no sólo averiguamos si las dos formas dadas son equivalentes, sino que hallamos además, al mismo tiempo, una sustitucion por la cual se convierte una de ellas en la otra. En efecto, al reducir la forma φ á la φ', y la ψ á la ψ' hallamos las trasformaciones respectivas S y T. Por lo tanto: si φ' y ψ' fuesen idénticas, y T' representara la sustitucion inversa de T, la forma φ se trasformaria en la ψ por la sustitucion compuesta ST'; y, si las formas φ' y ψ' no fuesen idénticas, pero sí equivalentes, y U designase la sustitucion, siempre hallada como vimos, por la cual se convierten una en otra, la forma φ se trasformaria en la ψ por la sustitucion compuesta SUT'.

Empero si las formas reducidas φ' y ψ', equivalentes á las propuestas, no fueran idénticas, ni estuviesen comprendidas en ninguno de los dos casos de equivalencia, definidos en el artículo anterior, no serian entre sí equivalentes, y lo mismo sucederia, por consecuencia, con las formas dadas φ y ψ.

En conclusion: los dos problemas fundamentales en la teoría de las equivalencias están ya resueltos para las determinantes negativas; pues en el procedimiento mismo para resolver el primero, esto es, para decidir si dos formas son, ó nó, equivalentes, hallamos, cuando las formas lo son, una sustitucion por la cual se convierte la una en la otra; y, hallada esta sustitucion, con arreglo al método explicado en los artículos (140) y (141), se deducen de ella todas las trasformaciones de la primera forma en la segunda: lo cual constituye precisamente el objeto del segundo problema.

147.—*Limitacion del número de clases para las formas correspondientes á una determinante negativa.*

La teoría de las formas reducidas nos proporciona tambien el medio de constituir un *sistema completo de formas no equivalentes* (138) para una determinante *negativa* dada: entendiéndose que tales formas tienen sus coeficientes extremos positivos (143). En efecto, como toda forma de determinante negativa $D = -\Delta$, es equivalente á una forma reducida, y, en general, á una sola, para obtener un sistema completo de formas, bastará encontrar todas las reducidas, cuidando, siempre que dos de éstas no sean idénticas, sino que se hallen comprendidas en alguno de los dos casos singulares de equivalencia señalados (145), de desechar una cualquiera de ellas y conservar la otra solamente.

Que, entre todas estas formas reducidas, es finito el número de las no-equivalentes, se desprende de las condiciones (143)

$$2(b) \leqq a, \quad a \leqq c, \quad (b) \leqq \sqrt{\tfrac{1}{3}\Delta}$$

á que están sujetos los coeficientes de una forma reducida (a, b, c). Para demostrarlo designemos por λ el máximo entero contenido en $\sqrt{\frac{1}{3}\Delta}$, en cuyo supuesto será $\lambda \leqq \sqrt{\frac{1}{3}\Delta} < \lambda + 1$. Dado el valor absoluto Δ, de la determinante D, el segundo coeficiente b, de la forma (a, b, c),

si ha de satisfacer á la condicion última de las arriba escritas, sólo podrá admitir los $2\lambda + 1$ valores siguientes:

$$0, \pm 1, \quad \pm 2, \quad \pm 3, \ldots\ldots \quad \pm \lambda.$$

Atribuyendo á b cualquiera de estos valores, los otros dos coeficientes, a, c, en virtud de la igualdad $ac = b^2 + \Delta$, se hallarán descomponiendo el binomio conocido, $b^2 + \Delta$, de todas las maneras posibles, en dos factores positivos: uno de los cuales, el menor, si no fueren iguales, representará el coeficiente a, y el otro el c, para que se cumpla la condicion $a \leqq c$. Satisfecha ya esta condicion en la forma así determinada (a, b, c), veremos si los valores asignados á sus coeficientes cumplen tambien con la otra condicion $2(b) \leqq a$: y, en caso afirmativo, dicha forma será reducida y la anotaremos, por consecuencia; desechándola en el contrario.

Con este proceder, y teniendo además en cuenta las precauciones al principio indicadas, es indudable que obtendremos todas las formas reducidas, *no-equivalentes*, de que es susceptible la determinante conocida $D = -\Delta$. Mas, por una parte, vemos que el número de valores que puede recibir el coeficiente b, es limitado; y, por otra, que tambien lo es el número de descomposiciones posibles de la cantidad $b^2 + \Delta$ para cada uno de aquellos valores de b: luego

El número de todas las formas reducidas, no equivalentes, para una determinante negativa, ó lo que es igual, *el número de clases de estas formas, es finito.*

Sirvan como aclaracion de lo que precede los siguientes ejemplos:

1.° Sea $D = -12$; y, por consecuencia: $\Delta = 12, \lambda = \sqrt{\frac{4}{3}\,12} = \sqrt{4} = 2$. Los valores asignables á b serán:

$$0, \pm 1, \pm 2$$

y los correspondientes del binomio $b^2 + \Delta$;

$$12, \quad 13, \quad 16.$$

Descompongamos estos últimos números de todas las maneras posibles en dos factores, á saber:

$$12 = 1.\ 12 = 2.\ 6 = 3.\ 4$$

$$13 = 1.\ 13$$

$$16 = 1.\ 16 = 2.\ 8 = 4.\ 4$$

Tomando siempre para valor de a el primero de los factores que figuran en las inmediatas descomposiciones, hallamos las once formas:

$$(1,\ 0,\ 12),\quad (2,\ 0,\ 6),\quad (3,\ 0,\ 4)$$

$$(1, \pm 1, 13)$$

$$(1, \pm 2, 16),\quad (2, \pm 2, 8),\quad (4, \pm 2, 4);$$

de las cuales no son reducidas, por no cumplirse en ellas la condicion $2(b) \leqq a$, las siguientes:

$$(1, \pm 1, 13),\quad (1, \pm 2, 16),\quad (2, \pm 2, 8).$$

Excluyendo éstas, quedan solamente:

$$(1, 0, 12),\quad (2, 0, 6),\quad (3, 0, 4),\quad (4, \pm 2, 4);$$

y, como las dos últimas $(4, +2, 4)$ y $(4, -2, 4)$, se hallan comprendidas en los dos casos singulares (145), desecharemos una de ellas, y restan, por fin, las cuatro:

$$(1, 0, 12),\quad (2, 0, 6),\quad (3, 0, 4),\quad (4, 2, 4).$$

Entre éstas, las dos solamente $(1, 0, 12)$ y $(3, 0, 4)$, son tambien primitivas, y ademas de primera especie, por no verificarse la congruencia $D \equiv 1 \pmod 4$.

2.° Sea $D=-35$; y, de consiguiente: $\Delta=35$, $\lambda=\left(\sqrt{\frac{4}{5}35}\right)=3$. Los valores posibles de b en este caso, serán:

$$0, \quad \pm 1, \quad \pm 2, \quad \pm 3:$$

y los correspondientes de $b^2+\Delta$ respectivamente:

$$35, \quad 36, \quad 39, \quad 44.$$

Descomponiendo estos números en dos factores como sigue:

$$35 = 1.\ 35 = 5.\ 7$$

$$36 = 1.\ 36 = 2.\ 18 = 3.\ 12 = 4.\ 9 = 6.\ 6$$

$$39 = 1.\ 39 = 3.\ 13$$

$$44 = 1.\ 44 = 2.\ 22 = 4.\ 11,$$

se obtienen, del modo ya conocido, 22 formas; entre las cuales sólo cumplen con la condicion $2(b) \leqq a$, las 10 siguientes:

$$(1, \quad 0, \quad 35), \quad (5, \quad 0, \quad 7), \quad (2, \pm 1, 18)$$

$$(3, \pm 1, 12), \quad (4, \pm 1, 9), \quad (6, \pm 1, \quad 6).$$

Entre éstas las dos $(2, \pm 1, 18)$, corresponden al primer caso, y las dos $(6, \pm 1, 6)$, al segundo de los singulares ya mencionados; así que, desechando una de cada par, quedan, por fin, las ocho formas reducidas, no equivalentes:

$$(1, \quad 0, \quad 35), \quad (5, \quad 0, \quad 7), \quad (2, 1, 18)$$

$$(3, \pm 1, 12), \quad (4, \pm 1, 9), \quad (6, 1, \quad 6)$$

que son todas además primitivas: las seis,

$$(1, 0, 35), \quad (5, 0, 7), \quad (3, \pm 1, 12), \quad (4, \pm 1, 9)$$

de primera especie; y las otras dos,

$$(2, 1, 18), \quad (6, 1, 6)$$

de segunda.

3.° Sea $D = -48$; y, por tanto: $\Delta = 48$, $\lambda = 4$. Los valores para b serán:

$$0, \pm 1, \pm 2, \pm 3, \pm 4;$$

y las descomposiciones de los correspondientes á la cantidad $b^2 + \Delta$:

$$48 = 1.\ 48 = 2.\ 24 = 3.\ 16 = 4.\ 12 = 6.\ 8$$

$$49 = 1.\ 49 = 7.\ 7$$

$$52 = 1.\ 52 = 4.\ 13$$

$$57 = 1.\ 57 = 3.\ 19$$

$$64 = 1.\ 64 = 2.\ 32 = 4.\ 16 = 8.\ 8$$

De las 25 formas que de estas descomposiciones se deducen sólo son reducidas las 11 siguientes:

$$(1, 0, 48), \quad (2, \ 0, \ 24), \quad (3, \ 0, \ 16), \quad (4, \ 0, \ 12)$$

$$(6, 0, \ 8), \quad (7, \pm 1, \ 7), \quad (4, \pm 2, 13), \quad (8, \pm 4, \ 8);$$

y, como los tres pares $(7, \pm 1, 7)$, $(4, \pm 2, 13)$, $(8, \pm 4, 8)$ constan de formas equivalentes, desechando una de cada uno de ellos, quedan solamente las 8 distintas:

$$(1, 0, 48), \quad (2, 0, 24), \quad (3, 0, 16), \quad (4, 0, 12)$$

$$(6, 0, \ 8), \quad (7, 1, \ 7), \quad (4, 2, 13), \quad (8, 4, \ 8).$$

De las cuales son primitivas de primera especie las 4,

$$(1, 0, 48), \quad (3, 0, 16), \quad (7, 1, 7), \quad (4, 2, 13),$$

y las otras 4 derivadas.

148.—*Representacion de los números por formas determinadas.*

Estudiados ya completamente los principios fundamentales que á las formas de determinante negativa se refieren, vamos á corroborar prácticamente, apoyados siempre en el de la permanencia de las leyes formales (17), la proposicion demostrada (139), con el exámen y discusion de algunas de aquellas formas cuyas determinantes sean números conocidos.

I. *De la determinante* $D = -1$.

Las formas con la determinante $D = -1$ constituyen una sola clase; pues á tal determinante, como fácilmente se percibe, corresponde una sola forma reducida, á saber:

$$(1, 0, 1) = x^2 + y^2.$$

Segun expresa esta forma, el problema que debemos resolver consiste en hallar los números m, susceptibles de ser descompuestos en dos cuadrados; debiendo concretarnos, si hemos de aplicar inmediatamente los principios establecidos, á las construcciones *propias* (x, y) de dichos números m, los cuales supondremos además, para mayor sencillez, que son *impares*.

Sea, pues, m un número impar, y desde luego positivo. Como la determinante $D = -1$ es resto cuadrático (139-*a*) de m, todos los factores primos contenidos en este número serán (112) de la forma $4h+1$. Y, recíprocamente: si tal sucede, $D = -1$ será resto cuadrático de m, y la congruencia

$$z^2 \equiv -1 \pmod{m}$$

contendrá 2^{μ} raices incongruentes (109), designando μ el número de factores primos, diferentes entre sí, contenidos en m, áun en el caso particular de ser $\mu = 0$ y $m = 1$. Siendo n la representante de una cualquiera de dichas raices, y, por consecuencia, $n^2 + 1 = m\,l$, tenemos ya constituida la forma (m, n, l) de determinante -1, la cual, como solamente existe una clase de formas para esta determinante, será equivalente por necesidad á la reducida $(1, 0, 1)$. Ahora bien, segun el procedimiento (144) hallamos una sustitucion por la que se convierte la forma $(1, 0, 1)$ en la (m, n, l); y de esta sustitucion, conforme se explicó en los artículos (141) y (142), se deducen todas las demas. Por otra parte el número de estas trasformaciones diferentes $\begin{pmatrix} x, \xi \\ y, \eta \end{pmatrix}$ (por ser $(1, 0, 1)$ primitiva de primera especie, y $(\Delta = 1)$ es (142) siempre 4: número igual al de construcciones (x, y) del dado m, que pertenecen á la raiz n; y, como lo mismo puede decirse de cada una de las 2^{μ} raices incongruentes de la congruencia anterior, resulta que el número total de construcciones (x, y), del número m por la forma $x^2 + y^2$, está expresado por el producto

$$4 . 2^{\mu} = 2^{\mu+2}.$$

Para averiguar ahora de cuántos modos diferentes puede ser descompuesto el número m en dos cuadrados, sin tener en cuenta el órden de éstos, ni el signo de sus raices, basta considerar que á cada *ocho* construcciones de la forma

$$(\pm x, \pm y) \quad \text{y} \quad (\pm y, \pm x),$$

corresponde *una* sola descomposicion $m = x^2 + y^2$; de lo cual se deduce que el número de estas descomposiciones diferentes es el total de construcciones, arriba escrito, dividido por ocho, esto es:

$$2^{\mu+2} : 2^3 = 2^{\mu-1};$$

con la única excepcion de $m = 1$; pues para este número 1 no existen ocho, sino *cuatro* construcciones distintas, á saber:

$$(\pm 1, 0) \quad \text{y} \quad (0, \pm 1)$$

que producen *una* sola descomposicion: $1 = 1^2 + 0^2$.

Es de advertir que de las ocho construcciones expresadas, las cuatro

$$(x, y), \quad (-x, -y), \quad (-y, x), \quad (y, -x)$$

pertenecen á una raiz; y las otras cuatro,

$$(x, -y), \quad (-x, y), \quad (-y, -x), \quad (y, x)$$

á la raiz de signo opuesto.

En el resultado general obtenido se comprende el caso particular siguiente:

Todo número primo positivo, de la forma $4h + 1$, *puede siempre descomponerse de un solo modo, en dos cuadrados.*

Casi supérfluo será notar que estos cuadrados no deben contener ningun factor comun.

Pero no lo es advertir que todo número positivo, de la forma $4h+1$, que pueda ser descompuesto de más modos, ó de ninguno, en dos cuadrados, no será de seguro número primo.

Ejemplo 1.° Sea $m = 37$, número primo de la forma $4h + 1$. La congruencia consiguiente $z^2 \equiv -1 \pmod{37}$, contiene (81) las dos raices $z = \pm 6$; eligiendo de éstas la $n = 6$, se obtiene la forma (37, 6, 1), que por la sustitucion $\begin{pmatrix} 0, +1 \\ -1, -6 \end{pmatrix}$ se convierte en la reducida (1, 0, 1); y ésta, á su vez, en aquella, por la sustitucion, inversa de la anterior, $\begin{pmatrix} -6, -1 \\ +1, \quad 0 \end{pmatrix}$. De donde resulta la descomposicion: $37 = 6^2 + 1^2$.

Omitimos escribir las cuatro construcciones, pertenecientes á la raiz 6, y las otras cuatro, pertenecientes á la raiz -6, por ser muy fácil de hacer despues de lo que antes al por menor dijimos.

En el mismo caso se encuentran los números:

$$5 = 1 + 2^2,\quad 13 = 2^2 + 3^2,\quad 17 = 1 + 4^2,\quad 29 = 2^2 + 5^2,$$

$$41 = 4^2 + 5^2,\quad 53 = 2^2 + 7^2,\quad 61 = 5^2 + 6^2,\quad 73 = 3^2 + 8^2,\ \text{etc.}$$

2.° Sea $m = 65 = 5.13$: producto de los dos números primos 5 y 13, de la forma $4h + 1$ ambos. En este caso, como $\mu = 2$, el número total de construcciones es $2^4 = 16$, y el de descomposiciones, por consecuencia, igual á 2. La congruencia consiguiente $z^2 \equiv -1 \pmod{65}$ contiene (109) las *cuatro* raices ± 8 y ± 18, con las cuales obtenemos las dos formas (65, 8, 1) y (65, 18, 5). De esta última se deduce: $b' \equiv -18 \pmod 5$, ó bien $b' \equiv -3 \pmod 5$, y, por tanto, $b' = 2$; y, en consecuencia, $b + b' = 20 = -a'\delta = -5\delta$, de donde sale $\delta = -4$.

Así hallamos la sustitucion $\begin{pmatrix} 0, & 1 \\ -1, & -4 \end{pmatrix}$, mediante la cual se convierte la forma (65, 18, 5) en la (5, 2, 1); y, como ésta no es reducida, estableceremos (144) de nuevo la congruencia $b'' \equiv -2 \pmod 1$ para determinar el valor de $b'' = 0$, y el consiguiente de $\delta = -2$; con los cuales se constituye la sustitucion $\begin{pmatrix} 0, & 1 \\ -1, & -2 \end{pmatrix}$, que trasforma la (5, 2, 1) en la (1, 0, 1) que es ya reducida. Luego la forma (65, 18, 5), por la sustitucion compuesta

$$\begin{pmatrix} 0, & 1 \\ -1, & -4 \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & -2 \end{pmatrix} = \begin{pmatrix} -1, & -2 \\ +4, & +7 \end{pmatrix},$$

se convierte en la reducida (1, 0, 1).

Del mismo modo hallamos, para la forma primera (65, 8, 1), la sustitucion $\begin{pmatrix} 0, & +1 \\ -1, & -8 \end{pmatrix}$ que la convierte en la reducida (1, 0, 1). Las sustituciones inversas de las dos anteriores, por las cuales esta forma reducida se convierte á su vez, respectivamente, en las dos formas (65, 8, 1) y (65, 18, 5) son las siguientes:

$$\begin{pmatrix} -8, -1 \\ +1, \quad 0 \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} +7, +2 \\ -4, -1 \end{pmatrix}:$$

de las cuales se derivan las descomposiciones que buscamos:

$$65 = 8^2 + 1^2 = 7^2 + 4^2.$$

Así se hallaria tambien:

$$221 = 5^2 + 14^2 = 10^2 + 11^2.$$

II. *De la determinante* $D = -2$.

Todas las formas, cuya determinante es $D = -2$, constituyen tambien una clase; pues sólo existe para dicha determinante una sola forma reducida, á saber:

$$(1, 0, 2) = x^2 + 2y^2.$$

Para encontrar los números *impares* m, representados por esta forma, lo primero es saber si la determinante $D = -2$ es resto cuadrático de m: para lo cual es necesario y suficiente que cada uno de los factores primos (impares) p, contenidos en m, satisfaga á la condicion

$$\left(\frac{-2}{p}\right) = +1;$$

y, por consecuencia (113), que p sea de la forma $8h+1$, ó de la $8h+3$. Recíprocamente: si los μ factores p, del número m, son de las formas $8h+1$, ú $8h+3$, la congruencia

$$z^2 \equiv -2 \pmod{m}$$

admitirá siempre 2^μ soluciones incongruentes. Designando por n un representante de estas raices, y estableciendo la igualdad $n^2+2 = ml$, la forma (m, n, l) será equivalente por precision á la $(1, 0, 2)$: y, por

lo tanto, hallamos (146) una sustitucion $\begin{pmatrix} x, & \xi \\ y, & \eta \end{pmatrix}$ mediante la cual se trasforma la última en la primera; pero existe ademas (141) otra sustitucion $\begin{pmatrix} -x, & -\xi \\ -y, & -\eta \end{pmatrix}$ con igual efecto: luego á la raiz elegida n, pertenecen *dos* construcciones diferentes (x, y) y $(-x, -y)$, del número m; siendo, por fin,

$$2 \cdot 2^{\mu} = 2^{\mu+1}$$

el número total de dichas construcciones.

Fácilmente se concibe tambien que, si las dos construcciones $\pm(x, y)$ pertenecen á la raiz n, las dos $\pm(x, -y)$ pertenecerán á la raiz $-n$; y, como cada *cuatro* de tales construcciones producen *una* sola descomposicion del número m, en un cuadrado y el duplo de otro, el conjunto de estas descomposiciones estará expresado por el cociente

$$2^{\mu+1} : 4 = 2^{\mu-1}.$$

Sólo hay que exceptuar el caso $\mu = 0$, y, en consecuencia, $m = 1$, para el cual las *dos* descomposiciones que resultan, por ser $+n \equiv -n \pmod{1}$, se reducen á la única: $1 = 1^2 + 2 \cdot 0^2$.

Comprendido en el problema general se halla el particular, muy interesante, que corresponde al valor $\mu = 1$, expresado en lenguaje vulgar como sigue:

Todo número primo p, de cualquiera de las formas $8h+1$ ú $8h+3$, puede ser descompuesto siempre y de una sola manera, en un cuadrado y el duplo de otro.

Ejemplos. 1.° Sea $m = 41$: número primo de la forma $8h+1$, para el cual es $\mu = 1$. Las dos raices de la congruencia consiguiente

$$z^2 \equiv -2 \pmod{41}$$

son ± 11: la forma $(41, 11, 3)$, por la sustitucion $\begin{pmatrix} -1, & -1 \\ +4, & +3 \end{pmatrix}$, se

convierte en la reducida $(1, 0, 2)$; y ésta, á su vez, en aquélla, por la sustitucion inversa $\begin{pmatrix} +3, & +1 \\ -4, & -1 \end{pmatrix}$: luego $x = 3$, $y = -4$; y, en conclusion:

$$41 = 3^2 + 2 \cdot 4^2.$$

2.° Sea $m = 33 = 3 \cdot 11$, tambien de la forma $8h + 1$, aunque no primo; y, por consecuencia, $\mu = 2$. La fórmula general da para este caso *dos* descomposiciones diferentes. En efecto, las cuatro raices de la congruencia

$$z^2 \equiv -2 \pmod{33}$$

son ± 8 y ± 14. Las dos formas correspondientes

$$(33, 8, 2) \quad \text{y} \quad (33, 14, 6),$$

mediante las sustituciones

$$\begin{pmatrix} -1, & 0 \\ +4, & -1 \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} -1, & +2 \\ +2, & -5 \end{pmatrix},$$

se convierten respectivamente en la reducida $(1, 0, 2)$. Las sustituciones inversas de las anteriores son:

$$\begin{pmatrix} -1, & 0 \\ -4, & -1 \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} -5, & -2 \\ -2, & -1 \end{pmatrix};$$

luego las dos descomposiciones del número 33 serán:

$$33 = 1^2 + 2 \cdot 4^2 = 5^2 + 2 \cdot 2^2.$$

III. *De la determinante* $D = -3$.

Para esta determinante existen *dos* clases de formas, cuyas representantes expresan las dos reducidas

$$(1, 0, 3) = x^2 + 3y^2$$

$$(2, 1, 2) = 2x^2 + 2xy + 2y^2$$

de la primera y la segunda especie respectivamente.

Por la primera forma sólo pueden ser construidos evidentemente números impares. Sea, pues, m un número impar y, para mayor sencillez, no divisible por 3; si ha de ser representado por la forma (1, 0, 3), es necesario que todo factor p contenido en dicho número m satisfaga á la condicion

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = +1,$$

para lo cual debe ser p de la forma $3h+1$. Y recíprocamente: cuando esta condicion se cumpla por todos los μ factores primos p, contenidos en m, la congruencia

$$z^2 \equiv -3 \pmod{m},$$

admitirá 2^μ raices incongruentes. Designando por n una representante de estas raices, y estableciendo la igualdad $n^2 + 3 = ml$, la forma (m, n, l) será de primera especie, puesto que m es impar, y equivalente, por consecuencia, á la reducida (1, 0, 3). Dos sustituciones,

$$\begin{pmatrix} x, & \xi \\ y, & \eta \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} -x, & -\xi \\ -y, & -\eta \end{pmatrix},$$

pueden hallarse, segun el artículo (141), para trasformar la forma (1, 0, 3) en la (m, n, l); y, *dos* construcciones, por lo tanto, (x, y) y $(-x, -y)$, del número m, pertenecientes á la raiz determinada n.

De donde se desprende que el número total de tales construcciones, diferentes, será

$$2 \cdot 2^{\mu} = 2^{\mu+1},$$

el cual se reduce á

$$2^{\mu+1} : 4 = 2^{\mu-1}$$

para las descomposiciones distintas de m en un cuadrado y el triplo de otro, con la única excepcion de $\mu = 0$, y, por tanto, $m = 1$.

Es digno de ser mencionado el caso particular siguiente:

Todo número primo, de la forma $3h + 1$, *puede ser descompuesto siempre y de un solo modo, en un cuadrado y el triplo de otro.*

Pasemos ahora á estudiar la segunda forma $(2, 1, 2)$. Los números construidos por esta forma deben ser necesariamente *pares;* y, concretándonos á los de la forma $2m$, en la cual representa m, como antes, un número impar, no divisible por 3, se prueba sencillamente que el conjunto de estos números m, es idéntico al de los considerados en el caso anterior; puesto que de la posibilidad de la congruencia $z^2 \equiv -3 \pmod{m}$ se deduce, entónces, que tambien es posible esta otra: $z^2 \equiv -3 \pmod{2m}$; y recíprocamente. Designemos por n' una representante de las 2^{μ} raices que puede admitir la última congruencia, y establezcamos la igualdad $n'^2 + 3 = 2ml$: la forma resultante $(2m, n', l)$, de segunda especie, por ser impar su coeficiente medio n' y par, en consecuencia, su tercero l, es equivalente de cierto á la dada $(2, 1, 2)$; y al probar esta equivalencia hallamos seis trasformaciones diferentes de la última forma en la primera; de las cuales se desprenden las *seis* construcciones

$$\pm(x, y),\ \pm(y, -x-y),\ \pm(x+y, -x),$$

pertenecientes á la raiz determinada n'; y, cambiando en éstas los primeros números constructores por los segundos, se obtienen las otras seis, pertenecientes á la raiz de signo opuesto $-n'$. Si, pues, cada raiz produce seis construcciones, el número

$$6 \cdot 2^{\mu} = 3 \cdot 2^{\mu+1},$$

expresará el total de construcciones del $2m$ por la forma $(2, 1, 2)$, ó lo que es igual, del m por la forma $x^2 + xy + y^2$. Mas, teniendo en cuenta que cada *cuatro* construcciones, de las formas

$$(x, y), \quad (-x, -y), \quad (y, x), \quad (-y, -x),$$

no pueden mirarse en rigor como diferentes, resulta que el número

$$3 \cdot 2^{\mu-1}$$

expresará el de construcciones esencialmente distintas.

De donde se infiere que para todo número primo $m = 3h + 1$, existen siempre tres construcciones diferentes mediante la forma $x^2 + xy + y^2$.

Merece notarse que entre los números $x, y, x + y$, siempre existe uno solo par; de modo que entre las seis construcciones del número $2m$ pertenecientes á la raiz n', existen siempre dos, $\pm(x', y')$, en las cuales será par $y' = 2u$. Haciendo además $x' + u = t$, la ecuacion $x'^2 + x'y' + y'^2 = m$ se convierte en esta otra $t^2 + 3u^2 = m$: es decir, se halla así una construccion $(t, u,)$, del número m por la forma $(1, 0, 3)$, perteneciente á la misma raiz n'.

Y en esto estriba el enlace entre las construcciones de los números m y $2m$ por las formas $(1, 0, 3)$ y $(2, 1, 2)$ respectivamente.

Ejemplo. Sea $m = 13$, número primo de la forma $3h + 1$. Las raices de la congruencia $2^2 \equiv -3 \pmod{2.13}$, y tambien las de la $z^2 \equiv -3 \pmod{13}$, son ± 7: las cuales (eligiendo la positiva) producen las dos formas

$$(13, 7, 4) \quad \text{y} \quad (26, 7, 2)$$

que por las sustituciones

$$\begin{pmatrix} -1, -1 \\ +2, +1 \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} 0, +1 \\ -1, -4 \end{pmatrix}$$

se convierte en las propuestas

$$(1, 0, 3) \quad \text{y} \quad (2, 1, 2).$$

Las dos sustituciones, inversas de las anteriores, son:

$$\begin{pmatrix} +1, +1 \\ -2, -1 \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} -4, -1 \\ -1, \quad 0 \end{pmatrix};$$

y de aquí se desprenden las construcciones:

$$13 = 1^2 + 3(-2)^2 = (-4)^2 + (-4).1 + 1^2$$

y de éstas las siguientes:

$$13 = 4^2 + 4.(-3) + (-3)^2 = 3^2 + 3.1 + 1^2.$$

IV.—*De la determinante* $D = -5$.

Para esta determinante existen dos formas reducidas, no equivalentes, ambas primitivas de la primera especie,

$$(1, 0, 5) \quad \text{y} \quad (2, 1, 3).$$

Vamos á determinar en el presente, del mismo modo que lo hicimos en los casos anteriores, el conjunto de los números m, impares y no divisibles por 5, que pueden ser construidos por dichas formas.

Para esto es ante todo necesario averiguar cuándo la determinante -5 será resto cuadrático de m; lo cual sucederá siempre que todo factor primo p, contenido en m, satisfaga á la condicion

$$\left(\frac{-5}{p}\right) = (-1)^{1/2(p-1)} \left(\frac{p}{5}\right) = +1$$

y, sea por consecuencia (121—II) y (116—4.°) de una de las cuatro formas

$$20h+1, \quad 20h+9, \quad 20h+3, \quad 20h+7.$$

Si así sucediere, la congruencia consiguiente

$$z^2 \equiv -5 \pmod{m}$$

contendrá 2^{μ} raices incongruentes, designando por μ, como repetidas veces lo hemos escrito, el número de los factores p, contenidos en m.

Llamando n á una representante determinada de estas raices, y haciendo $n^2+5=ml$, la forma resultante (m, n, l) será por necesidad equivalente á una sola de las dos formas reducidas, en un principio expresadas; existiendo entónces dos trasformaciones de esta forma reducida en la (m, n, l), y dos construcciones, por consecuencia, del número m por dicha forma reducida, pertenecientes á la raiz elegida n. De aquí se desprende inmediatamente que el número total de construcciones del número m, por las dos formas reducidas, posibles para la determinante dada, es

$$2 . 2^{\mu} = 2^{\mu+1}.$$

Pero resta averiguar, é igual duda ocurrirá siempre en circunstancias semejantes, por cuál de las dos formas reducidas, no equivalentes, que ahora se nos ofrecen, se habrán de verificar las dos construcciones pertenecientes á la raiz n, de que, sin distinguir, hemos hablado antes. Fácil es, sin embargo, desvanecer en el caso actual esta duda. En efecto, cuando el número m sea representado por la forma $(1, 0, 5)$, tendremos: $m=x^2+5y^2$, y, por tanto, $m \equiv x^2 \pmod 5$, esto es, m será resto cuadrático de 5; y, si al contrario, fuese m construido por la otra forma $(2, 1, 3)$, tendríamos: $m=2x^2+2xy+3y^2$, ó bien $2m=(2x+y)^2+5y^2 \equiv (2x+y^2) \pmod 5$; y, por consecuencia, como 2 es no resto de 5, m seria entónces no-resto de 5. De lo cual resulta que todas las construcciones del número m se efectuarán por la forma $(1, 0, 5)$ exclusivamente, ó por la forma $(2, 1, 3)$, segun que m sea resto, ó no-resto, del número 5: esto es, segun que sea $m \equiv \pm 1 \pmod 5$, ó $m \equiv \pm 2 \pmod 5$.

Inclusas en esta proposicion general se hallan las particulares siguientes:

Para todo número primo de una de las formas $20h+1$, *ó* $30h+9$, *existen cuatro construcciones por la forma* $(1, 0, 5)$ *que producen una sola descomposicion de dicho número en un cuadrado y el quintuplo de otro.*

Todo número primo, de una de las formas $20h+3$ *ó* $20h+7$, *puede ser construido de cuatro modos distintos por la forma* $(2, 1, 3)$.

Ejemplos. 1.° Sea $m=29$. Las dos raices de la congruencia $z^2 \equiv -5 \pmod{29}$ son $n = \pm 13$; tomando la representante $n=13$, se obtiene la forma $(29, 13, 6)$ que se convierte en la reducida $(1, 0, 5)$ por la sustitucion

$$\begin{pmatrix} -1, +1 \\ +2, -3 \end{pmatrix};$$

y de la sustitucion inversa se desprende la descomposicion

$$29 = 3^2 + 5 \cdot 2^2.$$

2.° Sea $m=27$: entónces $n = \pm 7$; y las dos formas consiguientes

$$(27, 7, 2) \quad \text{y} \quad (27, -7, 2)$$

se convierten en la reducida $(2, 1, 3)$ por las sustituciones

$$\begin{pmatrix} 0, +1 \\ -1, -4 \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} 0, 1 \\ 1, 3 \end{pmatrix}.$$

De las sustituciones inversas respectivamente se deducen las cuatro construcciones:

$$27 = 2(\mp 4)^2 + 2(\mp 4)(\pm 1) + 3(\pm 1)^2$$

$$27 = 2(\pm 3)^2 + 2(\pm 3)(\pm 1) + 3(\pm 1)^2;$$

de las cuales pertenecen á la raiz $+7$ las dos primeras, y á la raiz opuesta -7, las dos últimas.

No creemos necesario multiplicar más los ejemplos; en la tabla siguiente, relativa á las determinantes estudiadas y á algunas otras, en-

contrarán los lectores que lo desearen materia para ejercitarse en estas cuestiones.

Determinantes.	*Formas reducidas correspondientes.*
— 1	(1, 0, 1)
— 2	(1, 0, 2)
— 3	(1, 0, 3), (2, 1, 2)
— 5	(1, 0, 5), (2, 1, 3)
— 6	(1, 0, 6), (2, 0, 3)
— 7	(1, 0, 7), (2, 1, 4)
— 8	(1, 0, 8), (2, 0, 4), (3, 1, 3)
—10	(1, 0, 10), (2, 0, 5)
—11	(1, 0, 11), (2, 1, 6), (3, 1, 4), (3, —1, 4)
—12	(1, 0, 12), (2, 0, 6), (3, 0, 4), (4, 2, 4)

Esta tabla, como se ve, contiene solamente las formas positivas: esto es, aquellas cuyos coeficientes extremos son positivos; porque ya sabemos que una forma cualquiera, con la determinante — 1, por ejemplo, será equivalente á la reducida $(1, 0, 1) = x^2 + y^2$, si sus coeficientes extremos son positivos; y á la $-(x^2 + y^2)$, cuando fueren negativos. Y comprende, por consecuencia, la mitad de las representantes de las clases en que pueden distribuirse las formas pertenecientes á cada una de las determinantes no cuadradas, que le sirven de argumento. Esto prueba asimismo que entre las formas expresadas al lado de cada determinante no existirán dos que sean equivalentes en el sentido propio; aunque puedan serlo impropiamente, como sucede con las relativas á la determinante —11, entre las cuales se hallan las dos opuestas (3, 1, 4), (3, — 1, 4), que son impropiamente equivalentes, y nada más; en atencion á que, ni son ancípites, ni tienen iguales sus coeficientes extremos.

CAPITULO V.

Del primer problema fundamental de las equivalencias para las determinantes positivas.

Resueltos los dos problemas fundamentales (139) en la teoría de las equivalencias, para las formas de determinantes *negativas*, y hecha aplicacion de sus principios á la construccion de los números por dichas formas, en algunos casos particulares, vamos á estudiar ya los mismos problemas respecto de las formas con determinantes *positivas*.

En su lugar dijimos que el segundo de los problemas mencionados, á saber: *hallar todas las trasformaciones de una forma en otra, conocida una sola de aquellas trasformaciones*, se reducia en último extremo á determinar todas las soluciones enteras de la ecuacion

$$t^2 - Du^2 = \tau^2.$$

Y tambien oportunamente (Cap. III) expusimos las razones que nos obligaban á resolver este segundo problema antes que el primero.

Mas, tratándose de las formas con determinantes positivas, ofrecen estas dos cuestiones mayores dificultades; y esta circunstancia exije que invirtamos el órden seguido anteriormente, y que comencemos ahora por el exámen del primer problema: el de *averiguar si dos formas con determinantes iguales son, ó no, equivalentes;* cuya resolucion nos proporciona, en cambio, un ventajoso procedimiento para hallar por completo las soluciones de la ecuacion expresada.

149.—*Raices, primera y segunda, de una forma.*

En el método seguido ántes para exponer la doctrina de las formas con determinante negativa, no intervenian para nada los números *irra-*

cionales; el que adoptamos en nuestras actuales investigaciones difiere de aquél precisamente por el papel importante que en él representan dichos números: definámoslos, pues, ante todo, y fijemos claramente su sentido.

Sea

$$(a, b, c) = a x^2 + 2 b x y + c y^2$$

una forma, cuya determinante $b^2 - a c = D$ es positiva. Pues haciendo en ella $y : x = \omega$, la ecuacion resultante, de segundo grado,

$$a + 2 b \omega + c \omega^2 = 0,$$

tendrá las dos raices reales

$$\omega = \frac{-b \mp \sqrt{D}}{c} = \frac{a}{-b \pm \sqrt{D}}.$$

De estas dos raices se llama *primera* la que se refiere ó se halla expresada por el signo superior, y *segunda* la que resulta de tomar el signo inferior; y distinguiremos una de otra, presuponiendo de una vez para siempre que el radical $\sqrt{D}$ designe sin excepcion la raiz *positiva* de la determinante D. De este modo, cada una de las raices de la forma (a, b, c) puede ser determinada por los coeficientes de esta forma; y, recíprocamente: una forma se caracteriza por cualquiera de sus raices. Así que dos formas (a, b, c) y (a', b', c'), con la misma determinante D, serán idénticas necesariamente cuando sus raices primeras, ó segundas, sean iguales; pues de la igualdad que expresa esta última condicion,

$$\frac{-b' \mp \sqrt{D}}{c'} = \frac{-b \mp \sqrt{D}}{c},$$

ya se tomen los signos superiores, ya los inferiores, se desprende desde luego, por ser $\sqrt{D}$ irracional, que $c' = c$; y, entónces, $b' = b$, y por lo tanto, $a' = a$. Luego:

Dos formas, con la misma determinante positiva, serán idénticas siempre que una raiz de cualquiera de ellas coincida con la raiz del mismo nombre de la otra.

150.—*Dependencia entre las raices del mismo nombre, y de nombres distintos, de dos formas equivalentes.—Aplicacion á las formas contiguas.*

Sean (a, b, c) y (a', b', c') dos formas, propia ó impropiamente equivalentes, para comprender el caso en su más ámplio sentido; y $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ una sustitucion, ó trasformacion de la primera en la segunda, cuya determinante será, por consecuencia:

$$\alpha\delta - \beta\gamma = \varepsilon = \pm 1.$$

De la sustitucion admitida,

$$x = \alpha x' + \beta y', \qquad y = \gamma x' + \delta y',$$

dividiendo por x', se obtienen fácilmente las relaciones

$$\omega = \frac{\gamma + \delta\omega'}{\alpha + \beta\omega'} \qquad \text{y} \qquad \omega' = \frac{-\gamma + \alpha\omega}{\delta - \beta\omega},$$

mediante las cuales, como por dicha sustitucion se hacen idénticas las formas propuestas, puede evidentemente determinarse una raiz ω, de la forma (a, b, c), en funcion de una ω', de la forma (a', b', c'), y recíprocamente; en virtud de que tales raices son en realidad, como ya indicamos, los valores de las razones $y : x$ é $y' : x'$, para los cuales se convierten en cero las formas mencionadas.

Mas es indispensable, ante todo, averiguar si las dos raices, ω y ω', así relacionadas, son, ó no son, del mismo nombre, esto es: si son ambas primeras, ó segundas, ó si, por el contrario, una es primera y la

otra, segunda. Para esto sustituyamos en la expresion de ω', cambiados los signos, el valor de

$$\omega = \frac{-b \mp \sqrt{D}}{c}$$

y obtendremos la siguiente:

$$\omega' = \frac{\gamma c - \alpha(-b \mp \sqrt{D})}{-\delta c + \beta(-b \mp \sqrt{D})} = \frac{b\alpha + c\gamma \pm \alpha\sqrt{D}}{-b\beta - c\delta \mp \beta\sqrt{D}}$$

la cual, multiplicando sus dos términos por $-b\beta - c\delta \pm \beta\sqrt{D}$, se convierte en estas otras:

$$\omega' = \frac{-(b\alpha + c\gamma)(b\beta + c\delta) + \alpha\beta D \mp (\alpha\delta - \beta\gamma)c\sqrt{D}}{(b\beta + c\delta)^2 - \beta^2 D}$$

$$= \frac{-(a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta) \mp (\alpha\delta - \beta\gamma)\sqrt{D}}{a\beta^2 + 2b\beta\delta + c\delta^2}.$$

Y, teniendo presente que:

$$a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b'$$

$$a\beta^2 + 2b\beta\delta + c\delta^2 = c'$$

$$\alpha\delta - \beta\gamma = \varepsilon$$

resulta por fin:

$$\omega' = \frac{-b' \mp \varepsilon\sqrt{D}}{c'}.$$

De la comparacion de las expresiones para ω y ω' se desprende la ley que sigue:

Cuando una forma (a, b, c) *se convierta en otra equivalente* (a', b', c'), *por la sustitucion* $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$, *cualquiera raiz* ω, *de la primera, se halla ligada con cualquiera raiz* ω, *de la segunda, por las relaciones*

$$\omega = \frac{\gamma + \delta\,\omega'}{\alpha + \beta\,\omega'} \qquad \text{y} \qquad \omega' = \frac{-\gamma + \alpha\,\omega}{\delta - \beta\,\omega};$$

y estas dos raices, ω *y* ω', *serán además del mismo nombre, ó de nombres distintos, segun que la sustitucion expresada sea propia ó impropia.*

Excluyendo, pues, la equivalencia y la sustitucion impropias, resultará que siempre estarán enlazadas, del modo que se ha dicho, dos raices *del mismo nombre* de dos formas equivalentes.

La recíproca de la ley anterior es esta:

Cuando dos raices del mismo nombre, ω *y* ω', *de dos formas* (a, b, c) *y* (a', b', c'), *con igual determinante, se hallen enlazadas por la ecuacion*

$$\omega = \frac{\gamma + \delta\,\omega'}{\alpha + \beta\,\omega'},$$

y los cuatro números enteros $\alpha, \beta, \gamma, \delta$, *que en esta figuran, satisfagan á la condicion*

$$\alpha\,\delta - \beta\,\gamma = 1,$$

dichas formas serán equivalentes; convirtiéndose la primera en la segunda por la sustitucion $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$.

Para demostrar que esta proposicion recíproca es cierta, admitamos por un momento, que por la sustitucion $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ no se convierta la forma (a, b, c) en la (a', b', c'), sino en otra, equivalente por supuesto, (a'', b'', c''); y designemos por ω'' su raiz del mismo nombre que la ω. Segun la proposicion directa, estas dos raices ω y ω'' estarán ligadas por la ecuacion

$$\omega = \frac{\gamma + \delta\,\omega''}{\delta + \beta\,\omega''},$$

de la cual se desprende $\omega = \omega''$; y como, segun la hipótesis, ω' es del mismo nombre que ω, y, por consecuencia, que ω''; y, por otra parte, la forma (a', b', c') tiene la misma determinante que la (a, b, c), y, de consiguiente, la misma tambien que la (a'', b'', c''), conclúyese, de acuerdo con la ley final del párrafo anterior, que la forma (a', b', c') es idéntica á la (a'', b'', c''), ó lo que es igual, que la (a, b, c) por la sustitucion mencionada, se convierte realmente en la (a', b', c').

Es importante para lo sucesivo establecer tambien la relacion entre dos raices del mismo nombre de dos formas *contíguas*. Recordando (137-*a*) que para dos formas de este género (a, b, a') y (a', b', a''), se verifica la condicion $b + b' = -a'\,\delta$, y que es $\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$ la sustitucion por la cual se convierte la primera en la segunda, las relaciones que anteceden se trasforman en las siguientes:

$$\omega = \delta - \frac{1}{\omega'}; \quad \omega' = \frac{1}{\delta - \omega};$$

designando ω y ω', respectivamente dos raices del mismo nombre de las formas (a, b, a') y (a', b', a'').

151.—*Formas reducidas: propiedades de sus raices.*

La equivalencia entre las formas con determinante negativa no la establecimos directamente, sino por el intermedio de las formas llamadas *reducidas;* y de análoga manera debemos proceder ahora para tratar de averiguar cuándo dos formas con determinante positiva serán, ó no, equivalentes. Sólo que el concepto de las formas *reducidas,* que nos han de servir de intermediarias para fallar acerca de la equivalencia entre dos formas con determinante positiva, es esencialmente distinto del que

atribuimos á aquellas otras intermediarias, al estudiar la misma cuestion, referente á las formas con determinante negativa.

Comencemos por fijar bien la definicion, y propiedades consiguientes, de estas nuevas formas *reducidas.*

Una forma (a, b, c) *de determinante* D, *se llama reducida, cuando sus dos raices, primera y segunda, respecto de sus valores absolutos, satisfacen á las condiciones respectivamente*

$$\frac{-b-\sqrt{D}}{c}>1, \qquad \frac{-b+\sqrt{D}}{c}<1;$$

y, respecto de sus signos, los tienen opuestos una y otra.

De esta definicion se derivan las consecuencias siguientes:

1.ª Por ser el valor numérico de la primera raiz mayor que el de la segunda, la suma de los valores absolutos de las cantidades b y $\sqrt{D}$ será mayor que su diferencia; y, como $\sqrt{D}$ es siempre positiva, b será tambien positivo (pero no $=0$). Además, si las dos raices han de tener signos opuestos, deberán tenerlos tambien las cantidades

$$-(b+\sqrt{D}) \quad \text{y} \quad -b+\sqrt{D};$$

y, siendo la primera evidentemente negativa, deberá ser la otra positiva; para lo cual es indispensable que se verifiquen las condiciones:

$$0<b<\sqrt{D}.$$

Designando por (c) el valor absoluto del coeficiente c, y, teniendo ahora en cuenta los signos, serán:

$$\frac{b+\sqrt{D}}{(c)}>1 \quad \text{y} \quad 0<\frac{-b+\sqrt{D}}{(c)}<1;$$

de donde se desprenden las relaciones:

$$0<\sqrt{D}-b<(c)<\sqrt{D}-b.$$

Estas condiciones caracterizan completamente (*) las formas reducidas: pues de ellas, retrocediendo, se obtienen las que figuran en la definicion de tales formas.

2.ª Como $D = b^2 - ac$, y $b^2 < D$, el producto $-ac$ debe ser positivo; y para esto es necesario que los coeficientes a y c tengan signos opuestos. Pero la primera raiz tiene siempre signo opuesto al de c, y tambien al de la segunda raiz: luego la primera raiz y el primer coeficiente a, serán del mismo signo; é igualmente la segunda raiz y el tercer coeficiente c: como se infiere bien pronto de ser la diferencia $\sqrt{D} - b$ positiva.

3.ª A las mismas condiciones, antes establecidas para el valor absoluto del tercer coeficiente c, se halla sometido el valor absoluto del primero a. Porque de la igualdad

$$D = b^2 + (a)(c)$$

se deduce:

$$(a) = \frac{(\sqrt{D} + b)(\sqrt{D} - b)}{(c)}.$$

Y de las condiciones

$$\frac{\sqrt{D} + b}{(c)} > 1 \quad \text{y} \quad 0 < \frac{\sqrt{D} - b}{(c)} < 1,$$

las siguientes:

$$(a) > \sqrt{D} - b \quad \text{y} \quad (a) < \sqrt{D} + b.$$

De lo cual resulta que los coeficientes a y c, de la forma reducida (a, b, c), se hallan comprendidos entre los mismos límites $\sqrt{D} - b$ y $\sqrt{D} + b$; y, por consecuencia, si la forma (a, b, c) es re-

(*) Gauss. D. A., §. 183.

ducida, lo será tambien su *socia* (c, b, a); y, no siéndolo aquella, tampoco lo será ésta.

4.ª Interesa para lo sucesivo demostrar tambien que de las condiciones

$$\sqrt{D} - (a) < b < \sqrt{D} \quad \text{y} \quad (c) \geqq (a)$$

se desprende que la forma (a, b, c), de determinante D, es reducida; por más que la recíproca no sea cierta. Para ello basta dar á las condiciones precedentes la forma

$$0 < \sqrt{D} - b < (a) \leqq (c);$$

y así inmediatamente deducimos que la segunda raiz

$$\frac{-b + \sqrt{D}}{c}$$

es numéricamente < 1; y que la primera

$$\frac{-b - \sqrt{D}}{c'} = \frac{a}{\sqrt{D} - b}$$

es, en valor absoluto tambien, > 1. De estas propiedades de las raices se infiere, como antes, que b debe ser positivo; puesto que $\sqrt{D} + b$ es numéricamente mayor que $\sqrt{D} - b$; y, como además es $b < \sqrt{D}$, que las dos raices tienen signos opuestos.

152.—*Limitacion del número de formas reducidas para una determinante positiva, dada.*

De las propiedades características que, segun hemos visto en el párrafo anterior, se desprenden de la definicion de las formas reducidas,

resulta que *el número de dichas formas, para una determinante positiva, dada, es finito.*

En efecto, si por λ representamos el máximo entero contenido en $\sqrt{D}$, de tal modo que sea $\lambda < \sqrt{D} < \lambda + 1$, y, por consecuencia, λ por lo ménos $= 1$, el coeficiente $b < \sqrt{D}$, de la forma (a, b, c), siendo ésta reducida, sólo podrá recibir los λ valores diferentes $1, 2, 3, \ldots\ldots\lambda$; y el que para cada uno de estos valores tome la expresion $D - b^2 = (a)(c)$ habrá que descomponerlo, de todos los modos posibles, en dos factores: los cuales deberán estar comprendidos entre $\lambda - b$ y $\lambda + 1 + b$ exclusive, ó entre $\lambda + 1 - b$ y $\lambda + b$ inclusive; tener cada dos de ellos signos opuestos; y permutarse cuando sean desiguales, si hemos de formar todas las reducidas correspondientes á la determinante D. Y como el número de los valores de λ es finito, y lo es tambien el de las descomposiciones de $D - b^2$, lo será asimismo el de las formas reducidas, determinadas.

Ejemplos. 1.° Para $D = 13$, es $\lambda = 3$, y los valores de b, y descomposiciones correspondientes:

$b = 1 \quad D - b^2 = 12 = 3, 4$

$b = 2 \qquad\quad 9 = 3, 3$

$b = 3 \qquad\quad 4 = 1, 4 = 2, 2.$

Los cuales producen las 12 formas reducidas:

$$(\pm 3, 1, \mp 4), \quad (\pm 1, 3, \mp 4), \quad (\pm 3, 2, \mp 3)$$
$$(\pm 4, 1, \mp 3), \quad (\pm 4, 3, \mp 1), \quad (\pm 2, 3, \mp 2).$$

2.° Para $D = 19$ es $\lambda = 4$, y los valores de b y descomposiciones del número $D - b^2$, las que siguen:

$b = 1 \quad D - b^2 = 18$: no da descomposicion útil ninguna.

$b = 2 \qquad\quad 15 = 3, 5$

$b = 3 \qquad\quad 10 = 2, 5$

$b = 4 \qquad\quad 3 = 1, 3$

Con estos datos se constituyen las 12 formas reducidas:

$$(\pm 3, 2, \mp 5), \quad (\pm 2, 3, \mp 5), \quad (\pm 1, 4, \mp 3)$$

$$(\pm 5, 2, \mp 3), \quad (\pm 5, 3, \mp 2), \quad (\pm 3, 4, \mp 1).$$

3.° Para $D = 35$, es $\lambda = 5$, y por consecuencia:

$b=1$ $D-b^2 = 34$: no da descomposicion útil ninguna.

$b=2$ 31 »

$b=3$ 26 »

$b=4$ 19 »

$b=5$ $10 = 1.\ 10 = 2.\ 5.$

De donde se deduce que, para la determinante 35, existen solamente las 8 formas reducidas:

$$(\pm 1, 5, \mp 10), \quad (\pm 2, 5, \mp 5)$$

$$(\pm 10, 5, \mp 1), \quad (\pm 5, 5, \mp 2).$$

4.° Para $D = 79$ es $\lambda = 8$, y, por lo tanto:

$b=1$ $D-b^2 = 78$: no da descomposicion útil ninguna.

$b=2$ 75 »

$b=3$ $70 = 7.\ 10$

$b=4$ $63 = 7.\ 9$

$b=5$ $54 = 6.\ 9$

$b=6$ 43: no da ninguna descomposicion útil.

$6=7$ $30 = 2.\ 15 = 3.\ 10 = 5.\ 6$

$6=8$ $15 = 1.\ 15 = 3.\ 5.$

Y con estos datos se constituyen las 32 formas reducidas:

$$(\pm 7, 3, \mp 10),\quad (\pm 7, 4, \mp 9),\quad (\pm 6, 5, \mp 9),\quad (\pm 2, 7, \mp 15)$$

$$(\pm 3, 7, \mp 10),\quad (\pm 5, 7, \mp 6),\quad (\pm 1, 8, \mp 15),\quad (\pm 3, 8, \mp 5)$$

y

$$(\pm 10, 3, \mp 7),\quad (\pm 9, 4, \mp 7),\quad (\pm 9, 5, \mp 6),\quad (\pm 15, 7, \mp 2)$$

$$(\pm 10, 7, \mp 3),\quad (\pm 6, 7, \mp 5),\quad (\pm 15, 8, \mp 1),\quad (\pm 5, 8, \mp 3).$$

153.—*Equivalencia entre una forma de determinante positiva y otra reducida.*

—

Guardando toda la semejanza posible con la doctrina de las formas de determinante negativa, vamos á demostrar ahora tambien que

Toda forma con determinante positiva es equivalente á una forma reducida.

Y aquí lo mismo que antes (144) vamos á servirnos de las formas contíguas en la demostracion.

Sea (a, b, a') una forma dada, con determinante positiva. Para hallar la forma (a', b', a''), contígua de la propuesta, recordaremos (137-*a*) que el coeficiente medio, b', de esta nueva forma, sólo puede tener un valor $\equiv -b \pmod{a'}$, y no otro alguno. Si, pues, hallado el valor de b', vemos que satisface á las condiciones

$$\sqrt{D} - (a') < b' < \sqrt{D}$$

ya tenemos mucho adelantado para calificar á la forma (a', b', a'') de reducida. Pero dicho valor de b', determinado por la congruencia $b' \equiv -b \pmod{a'}$, se halla comprendido efectivamente entre los límites $\sqrt{D} - (a')$ y $\sqrt{D}$; pues los números enteros

$$\lambda + 1 - (a'),\ \lambda + 2 - (a'),\ \ldots\ldots\ \lambda - 1,\ \lambda$$

entre aquellos límites contenidos, constituyen un sistema completo de restos (mod. a'), entre los cuales se encontrará, y una sola vez, el valor de $b' \equiv -b \pmod{a'}$. Luego, si por la sustitucion ya conocida $\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$, en la cual $\delta = -(b+b') : a'$, trasformamos la forma (a, b, a') en su contígua $(a', b'\, a'')$, sólo nos resta averiguar si el tercer coeficiente de esta última forma satisface á la condicion (151-4.ª)

$$(a'') \geqq (a');$$

en cuyo caso la forma (a', b', a'') sería ya reducida, y la demostracion estaria terminada. Si no sucede así, y, por el contrario, es $(a') > (a'')$, calcularemos para la forma (a', b', a'''), como lo hicimos antes, su contígua (a'', b'', a'''), en la cual se verificarán desde luego las condiciones

$$\sqrt{D} - (a'') < b'' < \sqrt{D},$$

y veremos si tiene lugar la otra,

$$(a''') \geqq (a''),$$

que probaria ser la forma nueva (a'', b'', a'''), reducida. Y si esto no se verifica todavía, y, por el contrario, es $(a'') > (a''')$, seguiremos aplicando el mismo procedimiento hasta encontrar una forma $(a^{(n)}, b^{(n)}, a^{(n+1)})$ que sea reducida: y á esta tal forma vendremos á parar necesariamente despues de un número finito de trasformaciones, por ser finito el conjunto de los números inferiores á otro positivo, determinado, (a').

Conviene tener presente que, por el método explicado para obtener al fin una forma reducida, no logramos conocer directamente si antes de esta última forma hemos ya pasado por alguna que fuera reducida; pues, como ya indicamos (151-4.ª), existen formas de este género para las que no se verifican las condiciones especiales en dicho método empleadas. Mas, aparte de esto, el procedimiento anterior nos proporciona siempre, y es lo que realmente importa, una sustitucion, para convertir la forma dada en otra reducida, la cual está compuesta de las sustituciones sucesivas que en el mismo hayan ido presentándose.

Ejemplos. 1.° Sea la forma dada (4, 6, 7); su determinante $D=8$; y, por consecuencia, $\lambda=2$. Como en este caso es $(a')=7$, la série

$$\lambda+1-(a'),\ \lambda+2-(a'),\ \lambda+3-(a'),\ \lambda+4-(a'),\ \lambda+5-(a'),\ \lambda-1,\lambda$$

se convertirá en la numérica:

$$-4,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,$$

entre cuyos términos existe uno solo $\equiv -6 \pmod 7$ que es $1=b'$. La forma contígua de la propuesta será, por lo tanto (7, 1, — 1), que no es reducida; pero, como en ella es $(a'')=1$, se deduce en seguida $b''=\lambda=2$, y la forma nueva, contígua, (—1, 2, 4), que ya es reducida. La sustitucion para pasar de la forma dada á su contígua es $\begin{pmatrix} 0, +1 \\ -1, -1 \end{pmatrix}$; la sustitucion para pasar desde la segunda forma á la tercera y última es $\begin{pmatrix} 0, 1 \\ -1, 3 \end{pmatrix}$; y la sustitucion compuesta, que convierte la primitiva forma en la última, reducida, será, por consecuencia:

$$\begin{pmatrix} 1, +0 \\ -1, -1 \end{pmatrix} \begin{pmatrix} 0, 1 \\ -1, 3 \end{pmatrix} = \begin{pmatrix} -1, +3 \\ +1, -4 \end{pmatrix}.$$

2.° Para la forma (713, 60, 5) es $D=35$ y, por lo tanto, $\lambda=5$. Con estos datos se halla la forma (5, 5, — 2), contígua de la propuesta, pero en la que no se verifica la condicion $(a'')\geqq(a')$: por lo cual, siguiendo el método expuesto, pasamos á su contígua (— 2, 5, 5), que satisface á la condicion mencionada, y la declaramos, en consecuencia, reducida: debiendo de paso advertirse que lo era ya tambien la anterior (5, 5, — 2). La sustitucion compuesta de las dos sucesivas, para pasar de la forma primitiva á la (5, 5, — 2), y de ésta á la (— 2, 5, 5), mediante la cual se convierte la forma dada en esta última, reducida, es:

$$\begin{pmatrix} 0, +1 \\ -1, -13 \end{pmatrix} \begin{pmatrix} 0, 1 \\ -1, 5 \end{pmatrix} = \begin{pmatrix} -1, +5 \\ 13, -66 \end{pmatrix}.$$

3.° La forma (62, 95, 145), cuya determinante es $D = 35$, por las sustituciones sucesivas

$$\begin{pmatrix} 0, 1 \\ -1, 0 \end{pmatrix}, \quad \begin{pmatrix} 0, 1 \\ -1, 2 \end{pmatrix}, \quad \begin{pmatrix} 0, 1 \\ -1, 2 \end{pmatrix}, \quad \begin{pmatrix} 0, 1 \\ -1, 4 \end{pmatrix},$$

se convierte respectivamente en las formas

$$(145, -95, 62), \quad (62, -29, 13), \quad (13, 3, -2), \quad (-2, 5, 5);$$

de las cuales son reducidas la primera y la última. La sustitucion, compuesta de todas las anteriores, que trasforma en esta última la propuesta, es:

$$\begin{pmatrix} -3, +10 \\ +2, -7 \end{pmatrix}.$$

Demostrado plenamente que existe siempre una forma reducida, equivalente á cualquiera forma dada, con determinante positiva, y que el número de aquellas formas reducidas, para una determinante particular, es finito, conclúyese tambien que:

El número de clases de formas no-equivalentes, para una determinante positiva dada, es siempre finito.

Equivalencia entre dos formas reducidas.

Si fuera tan sencillo probar la equivalencia entre dos formas *reducidas*, no idénticas, con la misma determinante *positiva,* como entre dos formas *reducidas*, distintas, con igual determinante *negativa* (146), bien fácil sería tambien determinar la equivalencia entre dos formas, cualesquiera fuesen sus determinantes; pero esta cuestion es algo embarazosa, respecto de las determinantes positivas, y exige que vayamos estudiándola paso á paso hasta llegar á su solucion definitiva.

Comenzaremos por resolver el problema siguiente:

154.—*¿Existe siempre una forma, contígua de una reducida, que sea tambien reducida?*

Admitamos por de pronto que así suceda, y que $\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$ es la sustitucion consiguiente, por la cual se convierte la forma reducida (a, b, a') en su contígua por la derecha, y tambien reducida, (a', b', a''). Entónces las raices ω y ω', del mismo nombre, de cada una de estas dos formas respectivamente, se hallarán ligadas (150) por las ecuaciones

$$\omega = \delta - \frac{1}{\omega'} \quad \text{y} \quad \omega' = \frac{1}{\delta - \omega} = -\frac{1}{\omega - \delta}.$$

Supongamos, para mayor facilidad, que estas dos raices del mismo nombre son *primeras;* aunque las mismas relaciones existen entre las segundas. Como en toda forma reducida tienen signos opuestos los dos coeficientes extremos, y la primera raiz el mismo signo que el primer coeficiente, las dos fracciones *impropias*, ω y ω', tendrán respectivamente los mismos signos que a y a'; y, por consecuencia, *opuestos* entre sí: en atencion á que el primer coeficiente a', de la segunda forma, es al mismo tiempo el último de la primera. Despues de esto, de las ecuaciones anteriores se desprende que $\omega - \delta$ debe ser un quebrado *propio*, de igual signo que ω; y δ, por consecuencia, un entero completamente determinado: ya respecto de su valor absoluto, inmediatamente inferior al de ω; ya en cuanto á su signo, que coincide con el de esta raiz. De todo lo cual resulta que una forma reducida (a, b, a') tiene, á lo más, una contígua de ella por la derecha (a, b', a''), que es tambien reducida.

Mas, probado que la forma reducida (a, b, a'), *puede* tener una sola contígua por la derecha (a', b', a''), tambien reducida, ¿será posible demostrar además que esta forma (a', b', a'') existe realmente? Para contestar á esta pregunta, designemos, como antes, por ω la primera

raiz de la forma propuesta (a, b, a'), la cual será, por consecuencia, una fraccion impropia y del mismo signo que a; y determinemos el número δ de modo que su valor absoluto (δ), sea el máximo entero contenido en (ω) (nunca $= 0$), y su signo el mismo de ω. Por la sustitucion así determinada $\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$, se convertirá la forma (a, b, a) en una contígua, (a', b', a''), cuya primera raiz

$$\omega' = \frac{1}{\delta - \omega},$$

será un quebrado impropio, de signo contrario al comun de ω y a, é igual al de a'. Designando ahora por ω_1, y ω'_1, las dos segundas raices respectivamente de las formas (a, b, a') y (a', b', a''), entre ellas existirá, como sabemos, la relacion

$$\omega'_1 = \frac{1}{\delta - \omega_1};$$

de la cual, como ω_1 es un quebrado propio, de signo contrario al de ω, y, por lo tanto, al de δ; y δ es un entero diferente de cero, se desprende que $\delta - \omega_1$ es una fraccion impropia, y, en consecuencia, ω'_1 una fraccion propia, cuyo signo coincide con el comun de δ, ω, y a; y es opuesto al de ω' y a'. De donde se concluye que las dos raices, primera y segunda, ω' y ω'_1, de la nueva forma (a', b', a''), tienen signos opuestos, y además que la primera, ω', es un quebrado impropio, y otro quebrado, pero propio, la segunda ω'_1: condiciones que caracterizan á la forma (a', b', a'') de reducida. Luego:

Toda forma reducida tiene siempre una sola forma contígua por su derecha, que es tambien reducida, y puede hallarse fácilmente del modo que hemos explicado.

Siguiendo el anterior procedimiento pudiéramos demostrar además que para toda forma reducida existe una *sola*, contígua por su izquierda, que es asimismo reducida; pero es más sencillo fundar esta demostracion en el principio ya conocido (151-3.°) de que dos formas *socias*, (a, b, a') y (a', b, a), son simultáneamente reducidas, ó no reducidas.

En efecto, cuando la forma reducida, (a, b, a'), tenga una contígua

por su izquierda $('a, 'b, a)$, que sea tambien reducida, la socia de la primera, (a', b, a), y reducida, por consecuencia, tendrá la contígua por su derecha $(a, 'b, 'a)$, que será tambien reducida; y recíprocamente: si esta forma $(a, 'b, 'a)$, es contígua por la derecha de la forma reducida (a', b, a), y á su vez reducida, la $('a, 'b, a)$ lo será asimismo, y contígua además por la izquierda de la (a, b, a'): y, como acabamos de demostrar que para una forma reducida (a', b, a), sólo existe una, contígua por su derecha $(a, 'b, 'a)$, que es tambien reducida, resulta finalmente que:

Toda forma reducida tiene siempre una sola forma, contígua por su izquierda, que es tambien reducida.

155.—*Distribucion en períodos de las formas reducidas correspondientes á una determinante positiva.*

En conformidad con los principios demostrados, pueden todas las formas reducidas, correspondientes á una determinante positiva D, distribuirse en *períodos*, los cuales se formarán del modo siguiente:

Elíjase una forma reducida cualquiera φ_0, para la determinante dada, D, y marquemos con índices positivos sus contíguas reducidas, sucesivas, por la derecha, y con negativos las contíguas por la izquierda. La série constituida por estas formas,

$$\ldots\ldots \varphi_{-2}, \quad \varphi_{-1}, \quad \varphi_0, \quad \varphi_1, \quad \varphi_2 \ldots\ldots$$

está completamente determinada por la forma elegida φ_0, de la cual se deducen todas las demás, equivalentes con ella. Ahora bien, siendo finito el número de formas reducidas para una determinante D, claro es que todas las formas comprendidas en la série infinita, anterior, no podrán ser diferentes; y, por consecuencia, prolongando dicha série desde cualquiera de sus términos, por precision habremos de tropezar con otro, idéntico al que tomamos como punto de partida. El conjunto de formas ó términos distintos, que median entre uno de éstos y su próximo

idéntico se llama *período* de la forma fundamental de la série. Fijémonos en una forma ó término de esta série, φ_μ: siendo de signos opuestos los primeros coeficientes de dos formas ó términos consecutivos, tendremos que pasar por un número *par* $=2n$, de estos términos, hasta llegar á la forma $\varphi_{\mu+2n}$ idéntica á la elegida φ_μ; y, como cualquiera de las dos formas, φ_μ ó $\varphi_{\mu+2n}$, tiene una sola reducida, contígua por la derecha, y otra sola por la izquierda, las $\varphi_{\mu+1}$ y $\varphi_{\mu+1+2n}$, y tambien las $\varphi_{\mu-1}$ y $\varphi_{\mu-1+2n}$; y, en general, cada dos formas, entre cuyos índices exista la diferencia $2n$, serán asimismo idénticas. Luego en toda la série mencionada existirán á lo sumo $2n$ formas ó términos diferentes, á saber:

$$\varphi_0,\ \varphi_1,\ \varphi_2 \ldots\ldots \varphi_{2n-2},\ \varphi_{2n-1};$$

con tal que ninguna de las formas $\varphi_2,\ \varphi_4,\ \ldots\ldots\ \varphi_{2n-2}$ sea idéntica á la primitiva φ_0; porque, si fuesen idénticas, por ejemplo, φ_ν y $\varphi_{\nu+2r}$ lo serian tambien φ_{2r} y φ_0. Si admitimos, pues, que $2n$ es realmente el número de formas distintas, la série que las contiene se compondrá de este período con $2n$ formas, sucesiva é indefinidamente repetido, por derecha é izquierda, siendo idénticas cada dos formas, φ_μ y φ_ν, siempre que la diferencia de sus índices $(\mu - \nu)$ sea divisible por $2n$; y recíprocamente: cuando dos formas, φ_μ y φ_ν, sean idénticas, sus índices satisfarán á la congruencia $\mu \equiv \nu \pmod{2n}$.

Puede suceder que el período definido, de $2n$ formas, contenga precisamente todas las reducidas para la determinante propuesta D; pero tambien es posible lo contrario: esto es, que, además de las $2n$ existan para dicha determinante otras reducidas todavía. Designando, en este último caso, por ψ_0, una de las formas no contenidas en las que componen el período $2n$, no habria inconveniente en constituir un nuevo período con $2m$ formas,

$$\psi_0,\ \psi_1,\ \psi_2 \ldots\ldots \psi_{2m-2},\ \psi_{2m-1},$$

que serian entre sí diferentes, y diferentes tambien de las inclusas en el

primer período; pues, si los dos tuviesen una forma comun, esta última série y la primitiva, que sólo de un modo podrian entónces deducirse de tal forma comun, serian idénticas: contra lo supuesto.

Si todavía no estuviesen agotadas por los períodos $2n$ y $2m$, todas las formas reducidas, correspondientes á la determinante D, formaríamos un tercer período; y así proseguiríamos hasta concluir de agrupar en períodos todas las formas reducidas para la determinante dada.

El conjunto de estos períodos es necesariamente finito; y el número de términos que cada uno de ellos contenga podrá diferir de unos á otros, pero siempre, como se ha dicho, será par.

Ejemplos. 1.° En el artículo (152) hallamos el sistema de formas reducidas para la determinante $D = 13$. Tomando como punto de partida una de ellas, $(3, 1, -4)$, por ejemplo, se obtiene el siguiente período de 10 formas:

$$\varphi_0 = (3, 1, -4) \qquad \varphi_1 = (-4, 3, 1)$$

$$\varphi_2 = (1, 3, -4) \qquad \varphi_3 = (-4, 1, 3)$$

$$\varphi_4 = (3, 2, -3) \qquad \varphi_5 = (-3, 1, 4)$$

$$\varphi_6 = (4, 3, -1) \qquad \varphi_7 = (-1, 3, 4)$$

$$\varphi_8 = (4, 1, -3) \qquad \varphi_9 = (-3, 2, 3)$$

El cálculo de este período se efectúa como sigue. Ya dijimos que para hallar la forma (a', b', a'') contígua por la derecha de la (a, b, a') sólo teníamos que buscar su coeficiente medio b', completamente determinado por la congruencia $b' \equiv -b \pmod{a'}$, y las condiciones

$$\lambda + 1 - (a') \leqq b' \leqq \lambda,$$

y el cual es conocido inmediatamente por el sólo aspecto de la forma. En el ejemplo propuesto es $(a, b, a') = (3, 1, -4)$ y $\lambda = 3$; de modo

que el coeficiente b' de la forma φ_1 estará determinado por las condiciones

$$b' \equiv -1 \,(\text{mod. } 4), \quad 0 \leqq b' \leqq 3,$$

y será, por consecuencia, $b' = 3$. Hallado b', y despues $\delta = 1$, resulta:

$$a'' = \frac{b^2 - D}{a'} = a + (b - b')\,\delta = 3 + (1 - 3).\,1 = 1$$

y la forma $\varphi_1 = (-4, 3, 1)$. Ahora buscaríamos la forma contígua por la derecha de la ya conocida φ_1, y así continuaríamos hasta encontrar nuevamente la forma primitiva φ_0: lo cual ocurre en el ejemplo propuesto con la φ_{10}, contígua tambien por la derecha de la forma $\varphi_9 = (-3, 2, 3)$. Hallemos, pues, para verlo claramente dicha forma φ_{10}: su coeficiente medio $b^{(10)}$ estará determinado por las condiciones

$$b^{(10)} \equiv -2 \,(\text{mod. } 3), \quad 1 \leqq b^{(10)} \leqq 3,$$

y será, por lo tanto, $b^{(10)} = 1$; y, en consecuencia, $\delta = -1$, $a^{(11)} = -4$, y, al fin, $\varphi_{10} = (3, 1, -4) = \varphi_0$.

Pero las *diez* formas primitivas, de primera especie, que componen el período así hallado y antes escrito, no son todas las formas reducidas, correspondientes á la determinante 13; quedan fuera de él *dos* todavía, primitivas, de segunda especie,

$$\psi_0 = (2, 3, -2), \qquad \psi_1 = (-2, 3, 2),$$

que constituyen evidentemente un segundo período.

2.° Para la determinante $D = 19$, existen los dos períodos de seis términos cada uno:

$$\varphi_0 = (3, 2, -5) \qquad \varphi_1 = (-5, 3, 2)$$

$$\varphi_2 = (2, 3, -5) \qquad \varphi_3 = (-5, 2, 3)$$

$$\varphi_4 = (3, 4, -1) \qquad \varphi_5 = (-1, 4, 3)$$

y

$$\psi_0 = (-3, 2, 5) \qquad \psi_1 = (5, 3, -2)$$

$$\psi_2 = (-2, 3, 5) \qquad \psi_3 = (5, 2, -3)$$

$$\psi_4 = (-3, 4, 1) \qquad \psi_5 = (1, 4, -3)$$

3.° Para la determinante $D = 35$ los cuatro períodos, de dos términos cada uno:

$$\varphi_0 = (1, 5, -10) \qquad \varphi_1 = (-10, 5, 1)$$

$$\psi_0 = (10, 5, -1) \qquad \psi_1 = (-1, 5, 10)$$

$$\chi_0 = (2, 5, -5) \qquad \chi_1 = (-5, 5, 2)$$

$$\theta_0 = (5, 5, -2) \qquad \theta_1 = (-2, 5, 5)$$

4.° Por último, las 32 formas reducidas, correspondientes á la determinante $D = 79$, se distribuyen en cuatro períodos de á seis términos, y dos de á cuatro. Uno de los períodos de seis términos es el siguiente:

$$\varphi_0 = (7, 3, -10) \qquad \varphi_1 = (-10, 7, 3)$$

$$\varphi_2 = (3, 8, -5) \qquad \varphi_3 = (-5, 7, 6)$$

$$\varphi_4 = (6, 5, -9) \qquad \varphi_5 = (-9, 4, 7)$$

De este solo período se deducen fácilmente los otros tres. Para esto permútense los coeficientes extremos de la forma $\varphi_0 = (7, 3, -10)$, y resultará esta otra $(-10, 3, 7)$, á la cual, si se ha de conservar la contigüidad establecida, deberá seguir la φ_5 despues de efectuar en ella la misma permutacion; á la φ_5 la φ_4, con igual modificacion, etc. La permutacion de los coeficientes extremos en las formas del período escrito, por consecuencia, lleva consigo la inversion de derecha á izquierda en el órden de aquéllas.

Del modo que hemos dicho se obtiene un segundo período; y, mudando despues los signos á los coeficientes extremos de las formas contenidas, en cada uno de los dos períodos ya conocidos, obtendremos los otros dos períodos que buscábamos.

Uno de los de cuatro términos es el siguiente:

$$\psi_0 = (1, 8, -15) \qquad \psi_1 = (-15, 7, 2)$$

$$\psi_2 = (2, 7, -15) \qquad \psi_3 = (-15, 8, 1)$$

del cual se deduce el otro, cambiando los signos de los coeficientes extremos de sus términos.

155 *.—*Períodos de las formas socias, y ancípites.*

Entre las llamadas por Gauss (*) generales, todavía hay algunas observaciones acerca de los períodos definidos que merecen ser conocidas.

Ya dijimos (151-2.ª) que dos formas socias (a, b, a') y $(a' b, a)$ eran simultáneamente reducidas ó no reducidas; y tambien que, si para la forma reducida (a, b, a') existe una contígua por su izquierda, é igualmente reducida $('a, 'b, a)$, para la forma, socia de aquella y reducida (a', b, a), existirá tambien otra, contígua por su derecha $(a, 'b, 'a)$, que,

(*) Werke, t. I, pág. 170.

será asimismo reducida. Desarrollemos, pues, los períodos de las dos formas socias (a, b, c) y (c, b, a), y designémoslas, segun el lugar que en los mismos ocupan, respectivamente por φ_μ y ψ_ν. Conforme á los principios recordados, las dos formas $\varphi_{\mu+1}$ y $\psi_{\nu-1}$ serán tambien socias; y, en general, cada dos formas, $\varphi_{\mu+h}$ y $\psi_{\nu-h}$, siendo h un número entero: de donde resulta que los períodos correspondientes á las dos formas socias propuestas constan del mismo número de términos.

Gauss denomina tambien *períodos socios* á los períodos de las formas del mismo nombre.

Pero puede suceder más todavía, á saber: que los períodos socios sean idénticos, de modo que la forma misma ψ_ν, sea un término del período de la otra forma φ_μ; y entónces, evidentemente, las formas socias de cada una de las formas contenidas en este período serán tambien términos del mismo. Representemos, pues, por φ_ν la forma socia de la φ_0: en esta hipótesis, como los coeficientes extremos de toda forma reducida tienen signos opuestos, y los primeros coeficientes de las formas sucesivas de un período van siendo alternativamente positivos y negativos, el índice r de la forma φ_r tiene que ser por precision un número impar. Designémosle por $2m-1$, en conformidad con las observaciones expuestas: entónces las formas φ_0 y φ_{2m-1}, serán socias; lo mismo sucederá con las φ_h y φ_{2m-1-h}; con las φ_m y φ_{m-1}, por consecuencia; y tambien, si $2n$ es el número de términos del período, con las φ_{m+n} y $\varphi_{m-1-n} = \varphi_{m+n-1}$. Luego, representando por (A, B, C) cualquiera de las formas φ_m ó φ_{m+n}, su contígua por la izquierda será idéntica con la (C, B, A), y, por tanto, $2B \equiv 0 \pmod{A}$: lo cual quiere decir que las dos formas φ_m y φ_{m+n} son *ambíguas;* y diferentes además por no verificarse la congruencia $m \equiv m+n \pmod{2n}$.

En el período de cuatro términos antes expresado son *ancípites* las formas $(1, 8, -15)$ y $(2, 7, -15)$. Resumiendo cuanto precede, diremos en lenguaje vulgar que: *en todo período, socio de sí mismo, existen siempre dos formas ambíguas.*

Recíprocamente: si en un período cualquiera existe una forma ambígua (A, B, C), lo será tambien su contígua por la izquierda y socia,

(C, B, A): en cuyo caso, por consecuencia, no habrá una, sino dos formas ambíguas en el mencionado período. Luego: *ningun período puede contener una sola forma ambígua.*

Supongamos ahora que, además de las dos formas ambíguas φ_m y φ_{m+n} existe otra φ_s, en el mismo período. Por ser φ_s ambígua, las φ_{s-1} y φ_s, serán socias, y tambien las φ_{2s-1} y φ_0; la forma φ_{2s-1}, por lo tanto, será idéntica á la φ_{2m-1} y, en consecuencia, $2s \equiv 2m \pmod{2n}$, ó bien, $s \equiv m$, ó $s \equiv m+n \pmod{2n}$. Luego: *en un mismo período no puede haber más de dos formas ambíguas.*

En conclusion: los casos enumerados sólo pueden ocurrir evidentemente en el período de una forma que sea equivalente á su socia en el sentido propio, y, por consecuencia, impropiamente equivalente á sí misma, esto es, en el período de una forma perteneciente á una *clase ambígua.* Que, si la forma es de esta clase, en su período estará contenida tambien su socia, y, por lo tanto, existirán en el mismo dos formas ambíguas, se desprende de otra proposicion más general que demostraremos más adelante.

156.—*Desarrollo en fraccion contínua de las raices de las formas reducidas con determinante positiva.*

Las investigaciones precedentes, acerca de los períodos en que pueden distribuirse las formas reducidas para una determinante positiva, nos conducen como por la mano al desarrollo de las raices de estas formas en fraccion contínua. Elijamos para forma generativa, entre las de un período, aquella φ_0, cuyo primer coeficiente sea positivo: así será tambien su primera raiz ω_0. Designemos asimismo por ω_μ la primera raiz de la forma φ_μ; por δ_μ el cuarto coeficiente de la sustitucion

$$\begin{pmatrix} 1, & 0 \\ -i, & \delta_\mu \end{pmatrix}$$

que trasforma la φ_μ en su contígua por la derecha $\varphi_{\mu+1}$; y por k_μ el valor absoluto de dicho coeficiente δ_μ. Como este δ_μ tiene igual signo (154) que la raiz ω_μ, y su valor absoluto k_μ, coincide con el máximo entero contenido en el valor absoluto tambien de aquélla; y, por otra parte, las raices sucesivas $\omega_0, \omega_1, \omega_2, \ldots\ldots$ son alternativamente positivas y negativas, la cantidad $(-1)^\mu \omega_\mu$ será siempre positiva, y, en consecuencia:

$$k_\mu = (-1)^\mu \delta_\mu .$$

Entre las raices sucesivas $\omega_\mu, \omega_{\mu+1}, \omega_{\mu+2} \ldots\ldots$ existen las relaciones (150):

$$\omega_\mu = \delta_\mu - \frac{1}{\omega_{\mu+1}}, \qquad \omega_{\mu+1} = \delta_{\mu+1} - \frac{1}{\omega_{\mu+2}} ; \ldots\ldots$$

que, multiplicadas convenientemente por ± 1, ó ∓ 1, á fin de que sus primeros miembros sean siempre positivos, se convierten en estas otras:

$$\pm \omega_\mu = k_\mu + \frac{1}{\mp \omega_{\mu+1}} \qquad \mp \omega_{\mu+1} = k_{\mu+1} + \frac{1}{\pm \omega_{\mu+2}} \ldots\ldots$$

de las cuales se deduce para las fracciones impropias, positivas é irracionales $(-1)^\mu \omega_\mu$, la fraccion contínua infinita,

$$(-1)^\mu \omega_\mu = k_\mu + \cfrac{1}{k_{\mu+1} + \cfrac{1}{k_{\mu+2} + \ldots\ldots}}$$

que puede escribirse abreviadamente de este modo:

$$(-1)^\mu \omega_\mu = (k_\mu, k_{\mu+1}, k_{\mu+2}, \ldots\ldots).$$

Ahora bien, constando el período de las formas reducidas φ, de $2n$ términos, evidentemente será $\delta_{\mu+2n} = \delta_{\mu}$, y tambien $k_{\mu+2n} = k_{\mu}$: de lo cual se desprende que los términos k de la série infinita anterior se repiten por grupos, compuestos á lo sumo de $2n$ de aquellos; y, de consiguiente, que la fraccion contínua, equivalente á la raiz ω_{μ}, es *periódica*.

Ejemplos. 1.° Para la determinante $D = 13$ tomamos como forma generatriz la $(3, 1, -4) = \varphi_0$, de la cual dedujimos el período correspondiente (155). De las diez formas φ, contenidas en este período, mediante la igualdad $b^{(\mu)} + b^{(\mu+1)} = -a^{(\mu+1)}\delta_{\mu}$, deduciremos sucesivamente los valores del coeficiente δ_{μ}, á saber:

$$\delta_0 = +1, \quad \delta_1 = -6, \quad \delta_2 = +1, \quad \delta_3 = -1, \quad \delta_4 = +1$$

$$\delta_5 = -1, \quad \delta_6 = +6, \quad \delta_7 = -1, \quad \delta_8 = +1, \quad \delta_9 = -1.$$

Los valores absolutos correspondientes de δ_{μ} serán:

$$k_0 = 1, \quad k_1 = 6, \quad k_2 = 1, \quad k_3 = 1, \quad k_4 = 1$$

$$k_5 = 1, \quad k_6 = 6, \quad k_7 = 1, \quad k_8 = 1, \quad k_9 = 1$$

y la fraccion contínua, por consecuencia, equivalente á la primera raiz ω_0 de la forma $\varphi_0 = (3, 1, -4)$:

$$\omega_0 = \frac{1+\sqrt{13}}{4} = (1, 6, 1, 1, 1; 1, 6, 1, 1, 1, \ldots..)$$

Si consideramos ahora el otro período de dos formas, para la misma determinante,

$$\psi_0 = (2, 3, -2), \quad \psi_1 = (-2, 3, 2),$$

hallaremos por el mismo procedimiento:

$$\delta_0 = +3, \quad \delta_1 = -3:$$

y, de consiguiente:

$$k_0 = 3, \quad k_1 = 3,$$

de donde resulta que la primera raiz de la forma $\psi_0 = (2, 3, -2)$ es

$$\frac{3+\sqrt{13}}{2} = (3; 3; 3; \ldots\ldots)$$

Tanto respecto del período de las formas φ, como del de las ψ, nótase en este ejemplo, que el número de términos, en los períodos de las fracciones contínuas correspondientes, es la mitad del número de formas φ ó ψ que aquellos períodos contienen: circunstancia de la que hablaremos más adelante.

2.° Del período de seis formas para la determinante $D = 19$, se obtienen los valores siguientes:

$$\delta_0 = +1, \ \delta_1 = -3, \ \delta_2 = +1, \ \delta_3 = -2, \ \delta_4 = +8, \ \delta_5 = -2$$

$$k_0 = 1, \quad k_1 = 3, \quad k_2 = 1, \quad k_3 = 2, \quad k_4 = 8, \quad k_5 = 2;$$

y, por consecuencia:

$$\frac{2+\sqrt{19}}{5} = (1, 3, 1, 2, 8, 2; 1, 3, 1, 2, 8, 2; \ldots\ldots)$$

3.° Del período de seis términos, escrito para la determinante $D = 79$, se deducen:

$$\delta_0 = +1, \ \delta_1 = -5, \ \delta_2 = +3, \ \delta_3 = -2, \ \delta_4 = +1, \ \delta_5 = -1$$

$$k_0 = 1, \quad k_1 = 5, \quad k_2 = 3, \quad k_3 = 2, \quad k_4 = 1, \quad k_5 = 1,$$

y, por lo tanto:

$$\frac{3+\sqrt{79}}{10} = (1, 5, 3, 2, 1, 1; 1, 5, 3, 2, 1, 1; \ldots\ldots)$$

Del período de cuatro términos para la misma determinante resultan los valores:

$$\delta_0 = +1, \quad \delta_1 = -7, \quad \delta_2 = +1, \quad \delta_3 = -16$$

$$k_0 = 1, \qquad k_1 = 7, \qquad k_2 = 1, \qquad k_3 = 16;$$

y la primera raiz de la forma $\psi_0 = (1, 8, -15)$ será, por consecuencia:

$$\frac{8+\sqrt{79}}{15} = (1, 7, 1, 16; \ldots\ldots).$$

Por una permutacion ordenada y sencilla en los términos del período de esta fraccion contínua se hallan las correspondientes á las primeras raices de las otras tres formas $\psi_1 = (-15, 7, 2)$, $\psi_2 = (2, 7, -15)$ $\psi_3 = (-15, 8, 1)$, que son las siguientes:

$$-\frac{7+\sqrt{79}}{2} = -(7, 1, 16, 1; \ldots\ldots)$$

$$\frac{7+\sqrt{79}}{15} \qquad (1, 16, 1, 7; \ldots\ldots)$$

$$-\frac{8+\sqrt{79}}{1} = -(16, 1, 7, 1; \ldots\ldots)\ (*)$$

(*) La forma $(1, 0, -D)$ es equivalente á la reducida $\varphi_0 = (1, \lambda, \lambda^2 - D)$: desarrollando el período correspondiente á esta forma, la última de aquél será evidentemente $\varphi_{2n-1} = (\lambda^2 - D, \lambda, 1)$; y de aquí se desprende el desarrollo

$$\frac{1}{\sqrt{D}-\lambda} = (k_0, k_1 \ldots\ldots k_{n-2}, k_{n-1}, k_{n-2}, \ldots\ldots k_1, k_0, 2\lambda; \ldots\ldots)$$

y, por tanto:

$$\sqrt{D} = (\lambda; k_0, k_1 \ldots\ldots k_{n-2}, k_{n-1}, k_{n-2}, \ldots\ldots k_1, k_0, 2\lambda; \ldots\ldots)$$

Análogo desenvolvimiento ocurre siempre que existan en un período dos formas ambíguas (155*).—Véase el Apéndice I.

157.—*Conclusion del primer problema de las equivalencias para las formas de determinante positiva.*

Hemos demostrado que las raices de una forma reducida pueden desarrollarse en *fraccion contínua*; y, apoyándonos en las propiedades de las fracciones así determinadas, vamos ahora á resolver la cuestion fundamental de si dos formas reducidas, con la misma determinante, mas pertenecientes á distintos períodos, podrán ser, ó no, equivalentes: ó bien, si dos períodos diferentes de formas reducidas, para una determinante positiva podrán contener, ó no, formas equivalentes. Las propiedades de las fracciones contínuas, de las cuales depende cuanto á renglon seguido vamos á decir, no son, sin embargo, las más conocidas y vulgares, expuestas en los libros elementales de Algebra; sino otras de órden superior, que, para evitar largas digresiones en el cuerpo de la obra, hemos condensado al final, en el *Apéndice I*, y que, si el lector no conoce, debe imprescindiblemente tratar de comprender, antes de pasar más adelante. Dándolas ya por sabidas, es como vamos á continuar desenvolviendo el hilo de nuestros razonamientos.

Sean, pues, (a, b, c) y (A, B, C) dos formas reducidas y equivalentes en sentido propio. Como todas las formas de un mismo período son equivalentes entre sí, podemos admitir desde luego que los primeros coeficientes a y A, y, en consecuencia, las primeras raices de estas dos formas, son positivas; porque, de no ser así, de seguro se verificaria tal condicion en las formas inmediatamente contiguas á las propuestas. Hagamos, por abreviar, $(a, b, c) = \varphi_0$ y $(A, B, C) = \Phi_0$; y calculemos (155) para estas formas los períodos que las contienen; sus primeras raices respectivamente ω_0 y Ω_0, se desarrollarán en las fracciones contínuas regulares:

$$\omega_0 = (k_0 . k_1 . k_2 \ldots .$$

$$\Omega_0 = (K_0 . K_1 . K_2 \ldots . .$$

Por ser equivalentes las formas φ_0 y Φ_0 existirá siempre una trasformacion $\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}$ de la primera en la segunda, cuya determinante es

$$\alpha\delta - \beta\gamma = 1;$$

y, entre las raices primeras ω_0 y Ω_0 de aquellas formas, la relacion consiguiente

$$\omega_0 = \frac{\gamma + \delta\,\Omega_0}{\alpha + \beta\,\Omega_0}.$$

De las dos últimas ecuaciones, teniendo en cuenta que α no puede ser cero, porque entónces sería $A = c$, y, por consecuencia, A negativo, se desprende (*) la igualdad

$$\omega_0 = (\gamma', m, n, \ldots\ldots r, \beta', \Omega)$$

y, por lo tanto, esta otra:

$$\omega_0 = (\gamma', m, n, \ldots\ldots r, \beta', K_0, K_1, K_2 \ldots\ldots)$$

en cuya fraccion contínua infinita, á contar por lo ménos desde el término K_0, no existe irregularidad alguna, y el número de los elementos $\gamma', m, n, \ldots\ldots r, \beta'$ es par $= 2g$. Esta fraccion contínua será regular cuando β' sea positivo, porque entónces, como $\omega_0 > 1$, lo será tambien γ'; pero, si fuera $\beta' = 0$ ó negativo, se trasformará en regular, segun sabemos (*Apénd. I*). En tal conversion, tomando μ suficientemente grande, permanecerán invariables los elementos K_μ, $K_{\mu+1}$.....; y los anteriores á éstos, $\gamma', m, n, \ldots\ldots r, \beta', K_0, K_1 \ldots\ldots K_{\mu-1}$, en número de

(*) Apéndice I.

$(2g+\mu)$, serán sustituidos por otro número ν de elementos, cuya diferencia con el anterior $(2g+\mu)$ será par, esto es, $\nu \equiv \mu \pmod 2$, en virtud de que es positivo el valor de la fraccion entera. Ahora bien, como la raiz ω_0 puede desarrollarse de un solo modo en una fraccion contínua regular, los números

$$K_\mu, \quad K_{\mu+1}, \quad K_{\mu+2} \ldots\ldots$$

deben coincidir con los

$$k_\nu, \quad k_{\nu+1}, \quad k_{\nu+2} \ldots\ldots$$

Y, por consecuencia, si $\mu+h$ es un múltiplo del número de formas contenidas en el período de Φ_0, y número par, por lo tanto, el número $\nu+h$ será tambien par $=2m$, coincidiendo así los elementos

$$K_{\mu+h}, \quad K_{\mu+h+1}, \quad K_{\mu+h+2}, \ldots\ldots$$

con los

$$K_0, \quad K_1, \quad K_2 \ldots$$

y, de consiguiente, con los

$$k_{2m}, \quad k_{2m+1}, \quad k_{2m+2} \ldots\ldots$$

de lo cual resulta inmediatamente la igualdad

$$\Omega_0 = (k_{2m}, \; k_{2m-1}, \; k_{2m-2}, \ldots\ldots) = \omega_{2m}.$$

Pero toda forma se determina completamente, segun sabemos (149), por su raiz primera; y esto prueba, como expresa la última igualdad, que la forma Φ_0 debe ser idéntica á la φ_{2m}, y encontrarse, por consecuencia, entre las que constituyen el período de la φ_0. Luego:

Dos formas reducidas, equivalentes, con determinante positiva, pertenecen al mismo período; dos formas reducidas no serán equivalentes cuando pertenezcan á períodos distintos.

El método que de esta ley se desprende, para probar si dos formas dadas, con igual determinante positiva, son, ó no, equivalentes, es muy sencillo en teoría: se reduce á buscar dos formas reducidas, equivalentes respectivamente á las dos propuestas, y ver si las formas reducidas halladas pertenecen al mismo período, ó á períodos diferentes. En el primer caso habrá equivalencia; y por el procedimiento indicado se hallará tambien una sustitucion que convierte una de las formas en la otra; en el segundo, no serán equivalentes las dos formas dadas.

Ejemplo. Sean las formas (713, 60, 5) y (62, 95, 145) que tienen la misma determinante positiva $D = 35$. La primera por la sustitucion $\begin{pmatrix} 0, & 1 \\ -1, & -13 \end{pmatrix}$ se convierte en la reducida $(5, 5, -2)$; la segunda, por la sustitucion $\begin{pmatrix} -3, & +10 \\ +2, & -7 \end{pmatrix}$, en la reducida $(-2, 5, 5)$. Estas dos formas reducidas pertenecen al mismo período de dos términos

$$(5, 5, -2), \quad (-2, 5, 5)$$

y la primera se trasforma en la segunda por la sustitucion $\begin{pmatrix} 0, & 1 \\ -1, & 5 \end{pmatrix}$. Lo cual demuestra que las dos formas dadas son equivalentes; y, como la sustitucion $\begin{pmatrix} -7, & -10 \\ -2, & -3 \end{pmatrix}$ es la inversa de la $\begin{pmatrix} -3, & +10 \\ +2, & -7 \end{pmatrix}$, la primera se convertirá en la segunda por la sustitucion compuesta:

$$\begin{pmatrix} 0, & +1 \\ -1, & -13 \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 5 \end{pmatrix} \begin{pmatrix} -7, & -10 \\ -2, & -3 \end{pmatrix} = \begin{pmatrix} -3, & -5 \\ +41, & +68 \end{pmatrix}.$$

Dos palabras para concluir que no dejan de ser interesantes. Sabemos (137) que las formas *socias* son siempre en el sentido impropio equi-

valentes: luego, si las formas reducidas φ y Φ lo son tambien del mismo modo, y σ es la forma socia de φ, las formas Φ y σ serán equivalentes en el sentido propio, y, por lo tanto, la forma σ estará contenida en el período de la forma Φ. Mas, si las formas φ y Φ son propia é impropiamente equivalentes, es claro que, tanto φ como σ se encontrarán en el período de la forma Φ: por cuya razon este período será socio de sí mismo y contendrá dos formas ancípites, como ya demostramos. Y así se confirma además el teorema (155').

CAPITULO VI.

Del segundo problema fundamental de las equivalencias para las determinantes positivas.

158.—*Resolucion de la ecuacion de Pell para las determinantes positivas.*

En el artículo (142) resolvimos esta ecuacion, respecto de las determinantes negativas, dando por concluido allí el segundo problema fundamental de las equivalencias para dichas determinantes. Vamos á resolver ahora la misma ecuacion, respecto de las determinantes positivas, para terminar completamente tambien el segundo problema fundamental de las equivalencias, relativo á estas últimas determinantes, fundados en los principios que nos han servido para resolver el primero, explicados al por menor en el capítulo precedente.

Vamos, pues, á resolver la ecuacion

$$t^2 - D u^2 = \tau^2$$

en números enteros, para cualquier valor positivo, no cuadrado, de la determinante D.

Para esto recordemos ante todo la íntima conexion que existe entre la ecuacion anterior y el segundo problema de las equivalencias. Si (a, b, c) es una forma, con la determinante D y el divisor σ, y $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ una sustitucion propia, por la que se convierte aquella forma en sí misma, siempre se verificará el sistema de ecuaciones:

$$\alpha = \frac{t - b u}{\sigma}, \quad \beta = -\frac{c u}{\sigma}, \quad \gamma = \frac{a u}{\sigma}, \quad \delta = \frac{t + b u}{\sigma}$$

en las cuales representan t, u dos enteros determinados por la ecuacion arriba escrita. Cada solucion (t, u) de esta misma ecuacion produce, recíprocamente, mediante las últimas expresiones para $\alpha, \beta, \gamma \delta$, una sustitucion $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ que convierte en sí misma la forma (a, b, c).

Los principios, ya aludidos, expuestos en el artículo que antecede, nos proporcionan tambien, como veremos, el medio de encontrar directamente todas las trasformaciones $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ de una forma reducida, con la determinante positiva D, en sí misma; y, en consecuencia, todas las soluciones (t, u) de la ecuacion indeterminada de Pell. Pero antes de abordar de frente este asunto, debemos hacer algunas consideraciones, conducentes al mismo, acerca de los períodos de las formas reducidas.

Sabemos ya que la série de los elementos k, de la fraccion continua en que se desenvuelve la primera raiz ω_0, de una forma reducida φ_0, contiene un número par $= 2n$ de términos, á saber:

$$k_0, \quad k_1, \quad k_2, \ldots\ldots k_{2n-1};$$

que se repiten periódicamente; y que este número $2n$, es además el

de las formas reducidas, inclusas en un período juntamente con la φ_0. Pero hemos visto tambien, por el contrario, en algunos ejemplos, que los períodos de los números k, en las fracciones contínuas, equivalentes á las raices de las formas, constaban de un número de términos menor que el de las formas contenidas en el período correspondiente á una de ellas y del cual aquellos números k se derivaban: como acontece, por ejemplo, con el período de *diez* formas para la determinante 13, que sólo produce un período de *cinco* términos para los elementos k de la fraccion contínua; é importa mucho averiguar cuándo pueden ocurrir hechos semejantes.

Designemos para esto por $2n$, el número de los términos de un período de formas, y por m el de los términos de un período cualquiera en la série de los elementos k: entónces, conservando la notacion antes usada para las formas y sus raices, tendremos, *cuando m sea par:*

$$\omega_{m} = (k_{m}, k_{m+1}, \ldots) = (k_0, k_1 \ldots)$$

de donde $\omega_{m} = \omega_0$; φ_{m} será idéntica, por tanto, á φ_0, y m, en consecuencia, un múltiplo de $2n$; y esto prueba que en este caso no puede existir ningun período con un número par de términos k menor que el que expresa el de las formas de que los números k se derivan. Pero, *si m fuese impar*, siempre seria $2m$ tambien el número de términos de un período en la série de los números k, y, en consecuencia, múltiplo de $2n$, segun lo demostrado antes; para lo cual deberia ser m por lo ménos igual á n. Es decir que el caso de ser el período de los números k menor que el $2n$ de las formas correspondientes, sólo puede ocurrir cuando n sea impar; y entónces, como vimos en el ejemplo citado, el período de los números k puede constar de n términos; siendo además, por esta razon, $\omega_{n} = -\omega_0$, y, por consiguiente, $c_{n} = -c_0$, $b_{n} = b_0$, $a_{n} = -a_0$. No creamos, empero, que así sucederá siempre que n sea impar; pues tambien sabemos que los dos períodos de las formas correspondientes á la determinante $D = 19$, constan de seis términos cada uno, y es,

por lo tanto, $n = 3$; y el período consiguiente de los números k no se compone de 3, sino de 6 términos (*).

Para resolver ahora la ecuacion indeterminada $t^2 - D u^2 = \sigma^2$, en la cual D representa un número entero, positivo y no cuadrado, sujeto á una de las dos condiciones $D \equiv 0 \pmod{\sigma^2}$ ó $4D \equiv \sigma^2 \pmod{4\sigma^2}$, tomemos como punto de partida una forma *reducida* cualquiera (a, b, c).

(*) La circunstancia de que el número de términos del período en la fraccion contínua sea la mitad del número de las formas que constituyen tambien un período, se presenta sólo cuando las formas (a, b, c) y $(-a, b, -c)$ son equivalentes; y del artículo (157) se colige que así debe ocurrir siempre. Procediendo, para determinar la equivalencia de estas dos formas, como en el caso del artículo (141) encontramos ahora que los coeficientes de toda sustitucion, $\begin{pmatrix} \lambda, & \mu \\ \nu, & \rho \end{pmatrix}$, por la cual se convierte la forma (a, b, c), con la determinante D y el divisor σ, en la $(-a, b, -c)$, se hallan expresados por las fórmulas

$$\lambda = \frac{t - b u}{\sigma}, \quad \mu = \frac{c u}{\sigma}, \quad \nu = \frac{a u}{\sigma}, \quad \rho = -\frac{t + b u}{\sigma}; \qquad \text{(I}$$

donde t y u representan dos enteros que satisfacen á la ecuacion

$$t^2 - D u^2 = \sigma^2 \qquad \text{(II)}$$

Y, recíprocamente: deducidos estos números, t, u, las fórmulas (I) producen una sustitucion con la propiedad antes señalada: lo cual quiere decir que la circunstancia, de que antes hablamos, se presentará siempre y exclusivamente cuando la ecuacion (II) sea posible. Si tiene lugar en el período de una forma cualquiera, se verificará asimismo en todos los períodos de las formas pertenecientes al mismo *órden* (140); y, si además la ecuacion $t^2 - D u^2 = -1$ es posible, ocurrirá en los períodos de todas las formas que tengan la misma determinante D.

Esto último sucederá siempre que sea, por ejemplo, $D = p^{2s+1}$, y p un número primo $\equiv 1 \pmod{4}$. En efecto, designando por T, U la solucion *mínima* positiva de la ecuacion $T^2 - D U^2 = +1$, T será impar, U par, y

$$\frac{T-1}{2} \cdot \frac{T+1}{2} = D \left(\frac{U}{2} \right)^2.$$

con la determinante D y el divisor σ: forma que siempre existe, segun demostramos (140) y (153). Si admitimos además, en lo cual no hay inconveniente, que a sea positivo, y c entónces negativo, la primera raiz ω, de la forma supuesta (a, b, c), será positiva, y, por consecuencia:

$$\omega = (k_0, k_1 \ldots\ldots k_{2h-2}, k_{2h-1}, \omega)$$

designando $2n$ el número de términos del período de las formas, y h un entero cualquiera positivo. Estableciendo las igualdades

$$\frac{\gamma}{\alpha} = (k_0, k_1 \ldots\ldots k_{2h-2}), \quad \frac{\delta}{\beta} = (k_0, k_1 \ldots\ldots k_{2h-1})$$

será (*), segun la ecuacion tantas veces repetida, $\alpha\delta - \beta\gamma = 1$.

Ahora bien, como los dos factores del primer miembro de esta última ecuacion, por diferenciarse en una unidad, son primos entre sí, solo uno de ellos puede ser divisible por D. Si hacemos, pues, $T-1=2Df^2$, $T+1=2g^2$, $U=2fg$, resultará $g^2 - Df^2 = +1$, y $f < U$, contra lo supuesto de ser U el mínimo: luego deberemos establecer $T+1=2Dg^2$; $T-1=2f^2$, $U=2fg$, y entónces $t^2 - Dg^2 = -1$: que es lo que pretendíamos demostrar.

Dada la posibilidad de la ecuacion (II), se encuentran resultados notables examinando los períodos de las formas *ambíguas*. Para concretarnos al caso más sencillo, supongamos que la ecuacion

$$t^2 - Du^2 = -1$$

es resoluble. Si λ representa el máximo entero contenido en $\sqrt{D}$, la forma $\varphi_0 = (1, \lambda, \lambda^2 - D)$ será reducida y ambígua, con su período de $2n$ términos; y por consecuencia, n impar $= 2m+1$; $\varphi_{2m+1} = (-1, \lambda, D-\lambda^2)$, $\varphi_{2m} = (D-\lambda^2, \lambda, -1)$, de donde se deduce: $\varphi_m = (a, b, -a)$, $\varphi_{3m+1} = (-a, b, a)$; y, finalmente: $D = a^2 + b^2$; siendo a impar y primo con b, en virtud de que la forma φ_0 es primitiva de la primera especie. La descomposicion en dos cuadrados de un número primo $D \equiv 1 \pmod 4$, fué ya demostrada (148).

(*) Apéndice I.

$$\alpha = [k_1, \ldots\ldots k_{2hn-2}], \quad \beta = [k_1, \ldots\ldots k_{2hn-2}, k_{2hn-1}]$$

$$\gamma = [k_0, k_1 \ldots\ldots k_{2hn-2}], \quad \delta = [k_0, k_1 \ldots\ldots k_{2hn-2}, k_{2hn-1}]$$

$$\alpha + \beta\omega = [k_1, \ldots\ldots k_{2hn-2}, k_{2hn-1}, \omega]$$

$$\gamma + \delta\omega = [k_0, k_1, \ldots\ldots k_{2hn-2}, k_{2hn-1}, \omega]$$

de donde resulta:

$$\frac{\gamma + \delta\omega}{\alpha + \beta\omega} = (k_0, k_1 \ldots\ldots k_{2hn-2}, k_{2hn-1}, \omega).$$

Ahora bien, la forma (a, b, c), por la sustitucion $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$, se convierte en otra equivalente á ella; y entre las dos raices primeras, ω y ω', de una y otra forma, existe la relacion (150)

$$\omega = \frac{\gamma + \delta\omega'}{\alpha + \beta\omega'}$$

de la cual, y de la última igualdad se desprende que $\omega = \omega'$; y, como una forma está completamente determinada por su primera raiz, resulta finalmente que la forma (a, b, c) torna en sí misma por la sustitucion $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$.

Dando, pues, al entero h los valores sucesivos de la série natural $1, 2, 3, \ldots\ldots$ los numeradores y los denominadores de las reducidas correspondientes, que ocupan los lugares $2hn-1$ y $2hn$, constituirán una sustitucion $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ que convierte la forma (a, b, c) en sí misma (cuando $n=1$ y tomemos $h=1$, será $\alpha=1$, $\beta=k_1$, $\gamma=k_0$, $\delta=k_0 k_1+1$).

Los cuatro coeficientes $\alpha, \beta, \gamma, \delta$, son siempre positivos; y, por otra parte, los numeradores y los denominadores de las fracciones reducidas van creciendo constante y necesariamente á medida que h crece; y esto prueba que dos valores diferentes de h producen dos sustituciones $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ tambien diferentes.

Pero debemos demostrar tambien la recíproca, esto es: que del modo explicado se hallan *todas* las sustituciones $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$, que convierten en sí misma la forma (a, b, c), y cuyos coeficientes $\alpha, \beta, \gamma, \delta$, son todos *positivos*. Para esto representemos por $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ una cualquiera de estas sustituciones: desde luego se verificarán las ecuaciones

$$\alpha\delta - \beta\gamma = 1, \quad \omega = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}$$

de la última de las cuales resulta la siguiente:

$$\beta\omega^2 + (\alpha - \delta)\omega - \gamma = 0.$$

Esta ecuacion, como de segundo grado, tiene dos raices: una (151) de ellas, comprendida entre 1 y $+\infty$, y la otra entre -1, y 0: lo cual exige que su primer miembro sea negativo para $\omega = 1$, y positivo para $\omega = -1$, y, por consecuencia, que se verifiquen precisamente las desigualdades:

$$\gamma + \delta > \alpha + \beta \quad \text{y} \quad \beta + \delta > \alpha + \gamma.$$

Para hacer constar, como deseamos, que $\frac{\gamma}{\alpha}$ y $\frac{\delta}{\beta}$ son dos reducidas consecutivas de la fraccion contínua regular $(k_0, k_1, k_2, \ldots\ldots)$, debemos ante todo dejar sentado que $\gamma \geqq \alpha$ y $\delta > \gamma$; pero estas condiciones para los números γ, α, y δ, se desprenden inmediatamente de las desigualdades arriba escritas; pues, si fuese, contra lo estableci-

do, $\delta \leqq \gamma$, conforme á la segunda desigualdad, deberia ser $\alpha < \beta$, y tambien en consecuencia, $\alpha\delta < \beta\gamma$: resultado contradictorio de la igualdad $\alpha\delta - \beta\gamma = 1$ ó $\alpha\delta = \beta\gamma + 1$; luego, en efecto, $\delta > \gamma$; y, si fuese $\gamma < \alpha$, haciendo $\alpha = \gamma + \rho$ (siendo ρ entero positivo), segun lo exige la primera desigualdad deberia ser $\delta > \beta + \rho$, y, por consecuencia.

$$\alpha\delta - \beta\gamma > (\beta + \gamma)\rho + \rho^2:$$

relacion imposible por valer 1 su primer miembro, y 3, por lo ménos, su segundo, en virtud de que β, γ, ρ son enteros y positivos: luego efectivamente $\gamma \geqq \alpha$.

Síguese de lo dicho que no hay inconveniente en escribir la igualdad

$$\frac{\gamma}{\alpha} = (\gamma'. m. \ldots . q. r)$$

donde los elementos $\gamma', m, \ldots . q, r$, son todos positivos, y su conjunto es impar; porque está en nuestra mano resolver r en $r - 1 + \frac{1}{1}$ cuando así conviniere á nuestro intento.

Supongamos primeramente que $\alpha > 1$; como, segun acabamos de probar, $\gamma > \alpha$, y además γ no es divisible por α, la fraccion contínua igual á la ordinaria $\gamma : \alpha$, comprenderá, por lo ménos, tres elementos. Formemos la reducida inmediatamente anterior á la $\gamma : \alpha$,

$$\frac{\varphi}{f} = (\gamma'. m. \ldots . q):$$

de lo expuesto antes, y de las relaciones consiguientes $\alpha\varphi - f\gamma = 1$, $\alpha\delta - \beta\gamma = 1$, se deducen $\beta = f + \alpha\beta'$, $\delta = \varphi + \gamma\beta'$, siendo β' entero y *positivo;* pues, si fuera $\beta' = 0$, seria $\delta = \varphi$, y, como siempre $\varphi < \gamma$, resultaria $\delta < \gamma$: contra lo demostrado; y, si fuese β' negativo, δ seria negativo: contra lo supuesto en un principio de ser los cuatro números $\alpha, \beta, \gamma, \delta$ enteros y positivos. Luego tambien podemos establecer la igualdad

$$\frac{\delta}{\beta} = (\gamma'. m. \ldots . q. r. \beta'):$$

y, por consecuencia, como antes:

$$\omega = \frac{\gamma + \delta\,\omega}{\alpha + \beta\,\omega} = (\gamma', m, \ldots\ldots q, r, \beta', \omega)$$

donde los elementos $\gamma', m, \ldots\ldots q, r, \beta'$, son enteros y positivos, y su número par. Conclusion, por otra parte, que se desprende inmediatamente de que, segun las desigualdades que nos han servido de base para llegar á ella, los máximos enteros γ' y β', contenidos en las fracciones $\gamma : \alpha$ y $\beta : \alpha$, respectivamente, son positivos.

Supongamos ahora que es $\alpha = 1$: entónces inmediatamente:

$$\omega = \frac{\gamma + (\beta\,\gamma + 1)\,\omega}{1 + \beta\,\omega} = (\gamma, \beta, \omega):$$

resultado enteramente análogo al anterior.

Conclúyese de cuanto precede que siempre podremos desarrollar la raiz ω en una fraccion contínua periódica, regular,

$$\omega = (\gamma', m, \ldots\ldots q, r, \beta'; \gamma', m, \ldots\ldots)$$

en la cual sea par el número de los elementos $\gamma', m, \ldots\ldots q, r, \beta'$. Y como, por un lado, los números $\gamma', m, \ldots\ldots$ deben coincidir respectivamente con los $k_0, k_1 \ldots\ldots$; porque solo de un modo puede ser la raiz ω desarrollada en fraccion contínua; y, por otro, hemos demostrado que todo período de los números k, con un número par de términos, ó es idéntico á la série de los mismos números k correspondientes á todas las $2n$ formas, ó se compone de este mínimo período de un número par $= 2n$ de términos, varias veces repetido, serán $r = k_{2hn-2}$, $\beta' = k_{2hn-1}$, representando h un entero cualquiera positivo; y, por consecuencia:

$$\frac{\gamma}{\alpha} = (k_0, k_1, \ldots\ldots k_{2hn-2}), \qquad \frac{\delta}{\beta} = (k_0, k_1 \ldots\ldots k_{2hn-2}, k_{2hn-1})$$

que es lo que pretendíamos demostrar.

Explicado cómo pueden hallarse todas las trasformaciones de una forma en sí misma, mediante los cuatro coeficientes positivos, $\alpha, \beta, \gamma, \delta$, en el supuesto de ser tal forma reducida y su primer coeficiente tambien positivo, detengámonos ahora un poco en examinar las expresiones conocidas de estos cuatro coeficientes positivos, con ánimo de patentizar, mediante ellas, que las soluciones correspondientes $(t, u,)$ de la ecuacion de Pell, constan asimismo de dos términos *positivos*. Las expresiones mencionadas son:

$$\alpha = \frac{t - b u}{\sigma}, \quad \beta = -\frac{c u}{\sigma}, \quad \gamma = \frac{a u}{\sigma}, \quad \delta = \frac{t + b u}{\sigma}.$$

Como el primer coeficiente a de la forma (a, b, c) es positivo, que lo es u se desprende inmediatamente de la tercera fórmula; y de las desigualdades $\delta > \gamma$ y $\gamma \geqq \alpha$, antes demostradas, y de la que de ellas se deriva, $\delta > \alpha$, que tambien t es positivo. Mas recíprocamente: si t, u son dos números *positivos* que verifican la ecuacion de Pell, la sustitucion que con ellos se forma $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$, consta de cuatro números *positivos*. Efectivamente, siendo reducida la forma (a, b, c), su coeficiente medio b es positivo; y como por hipótesis lo es su primero a, y en consecuencia, su último c negativo, se colige de las expresiones recordadas, que β, γ, δ son positivos. Para demostrar que tambien lo es α, nos fijaremos en que $t^2 - b^2 u^2 = \sigma^2 - a c u^2$ es una cantidad positiva; y, como $t^2 - b^2 u^2 = (t + b u)(t - b u)$, es necesario que $t - b u$, y α, por consecuencia, tenga el mismo signo que $t + b u$, el cual es evidentemente positivo.

159.—*Solucion mínima de la ecuacion de Pell. Fórmula general.*

Todas las soluciones de la ecuacion de Pell, constituidas por dos números enteros y positivos, t, u, pueden encontrarse, conforme á la doctrina del artículo precedente, desenvolviendo en fraccion contínua

la raiz ω de la forma (a, b, c). Mas, por otra parte, de la forma misma de la ecuacion dicha se desprende que los valores de t y u crecen ó menguan simultáneamente; lo mismo acontece, como sabemos, con los numeradores y denominadores de las fracciones reducidas; y, por consecuencia, el valor de u y el de su compañero t, crecerán al mismo tiempo que γ, y por lo tanto, que el número h. Así que, tomando $h=1$, la solucion correspondiente la formarán los *mínimos* valores T, U que pueden recibir respectivamente las incógnitas t y u; contando con que la solucion $t=\sigma$, $u=0$ no pertenece á las soluciones positivas.

Vamos á probar ahora, primeramente, que es muy fácil hallar esta solucion *mínima* (T, U), mediante un período de una forma reducida, como se colige de lo que acabamos de decir; y despues, que de esta solucion mínima pueden deducirse todas las demás.

I. Para el primer extremo, ya teóricamente demostrado, sólo pondremos un par de ejemplos.

1.° Sea la determinante $D=79$. Una de las formas reducidas pertenecientes á esta determinante, la que tomamos (155-4.°) como generatriz de uno de los períodos, es la $(7, 3, -10)$, de primera especie. Del período correspondiente se dedujeron los números

$$k_0=1,\ k_1=5,\ k_2=3,\ k_3=2,\ k_4=1,\ k_5=1$$

ó elementos de la fraccion contínua $(1, 5, 3, 2, 1, 1)$. Las reducidas de esta fraccion son:

$$\frac{1}{1},\quad \frac{6}{5},\quad \frac{19}{16},\quad \frac{44}{37},\quad \frac{63}{53},\quad \frac{107}{90}$$

y los términos de las dos últimas, por consecuencia, componen la sustitucion $\begin{pmatrix}53, & 90\\ 63, & 107\end{pmatrix}$ de la forma $(7, 3, -10)$ en sí misma. Ahora bien, si solo queremos hallar la solucion mínima de la ecuacion $t^2-Du^2=\sigma^2$, bastará formar los denominadores de las reducidas hasta $\beta=90$, ó los numeradores hasta $\gamma=63$; y por las fórmulas $\beta\sigma=-cu$, ó $\gamma\sigma=au$, se halla el menor de los números u, á saber: $U=9$, del cual se de-

duce el correspondiente $T=\sqrt{(\sigma^2+DU^2)}=\sqrt{(1+79.81)}=\sqrt{6400}=80$. Tambien podria calcularse T por las fórmulas $a\sigma+bU$, ó $\delta\sigma-bU$.

Si tomásemos, como punto de partida, la forma $(1, 8, -15)$, tendríamos:

$$k_0 = 1,\ k_1 = 7,\ k_2 = 1,\ k_3 = 16.$$

Las reducidas consecutivas de la fraccion contínua $(1, 7, 1, 16)$ son:

$$\frac{1}{1},\quad \frac{8}{7},\quad \frac{9}{8},\quad \frac{152}{135},$$

y las dos últimas producen la sustitucion $\begin{pmatrix}8, & 135\\ 9, & 152\end{pmatrix}$, de donde resulta la misma solucion mínima que antes: $U=9,\ T=80$.

2.° Sea $D=13\equiv 1 \pmod 4$. Para hallar en este caso la solucion mínima de la ecuacion $t^2-13u^2=4$, elegiremos la forma reducida $(2, 3, -2)$ que arroja los números

$$k_0 = 3,\ k_1 = 3.$$

Las reducidas consiguientes son

$$\frac{3}{1},\quad \frac{10}{3},$$

de las cuales se desprende la sustitucion $\begin{pmatrix}1, & 3\\ 3, & 10\end{pmatrix}$, y de aquí la solucion que buscamos: $U=3,\ T=11$.

II. Cuanto respecta al primer punto está terminado: veamos ahora cómo de la *mínima* pueden deducirse todas las soluciones (t, u) de la ecuacion de Pell.

Sean t, u dos números cualesquiera, positivos ó negativos, que satisfagan á la ecuacion dicha,

$$t^2-Du^2=(t+u\sqrt{D})(t-u\sqrt{D})=\sigma^2$$

y designemos las dos expresiones correspondientes

$$\frac{t+u\sqrt{D}}{\sigma} \quad \text{y} \quad \frac{t-u\sqrt{D}}{\sigma},$$

para entendernos mejor, con los nombres respectivos de factores, *primero* y *segundo*, teniendo presente que $\sqrt{D}$ se considera siempre como positivo. Es evidente que el producto de estos dos factores es igual á 1; y, por consecuencia, ambos tendrán el mismo signo, que será positivo, ó negativo, segun que t sea positivo ó negativo. Por otra parte, cuando t y u tengan signos iguales, el *primer* factor será numéricamente mayor que el segundo, y, por tanto, >1; al paso que el *segundo* será, en valor absoluto, <1; lo contrario sucederá cuando los signos de t y u sean opuestos; y los dos factores serán iguales á ± 1, cuando $u=0$. Luego, si los números t y u son positivos, el primer factor, correspondiente á tal solucion, será un quebrado impropio, positivo; y recíprocamente: si este primer factor es un quebrado impropio, positivo, los dos números, t y u, serán tambien positivos.

Hecha esta consideracion preliminar, representemos por (t', u') y (t'', u'') dos soluciones cualesquiera, idénticas ó diferentes, de la ecuacion que estamos analizando: el producto de los dos primeros factores, correspondientes á cada una de aquellas,

$$\frac{t'+u'\sqrt{D}}{\sigma} \cdot \frac{t''+u''\sqrt{D}}{\sigma} = \frac{t+u\sqrt{D}}{\sigma}$$

en el cual

$$t = \frac{t'\,t''+D\,u'\,u''}{\sigma}, \qquad u = \frac{t'\,u''+u'\,t''}{\sigma},$$

representa una nueva solucion (t, u). En efecto, de los valores atribuidos á los números t y u, ó cambiando $\sqrt{D}$ en $-\sqrt{D}$ en la ecuacion de donde se derivan, resulta la siguiente:

$$\frac{t'-u'\sqrt{D}}{\sigma} \cdot \frac{t''-u''\sqrt{D}}{\sigma} = \frac{t-u\sqrt{D}}{\sigma}.$$

y, multiplicando una por otra, la propuesta:

$$t^2 - Du^2 = \sigma^2.$$

Lo que debemos inquirir, por lo tanto, es si los valores de t y u son enteros (condicion indispensable para que representen una solucion de la ecuacion última), ya sea $D \equiv 0 \pmod{\sigma^2}$, ya $4D \equiv \sigma^2 \pmod{4\sigma^2}$; y para esto es suficiente probar que lo es u; porque, siéndolo u, de la misma ecuacion se deduce que t^2, y, de consiguiente, t es tambien número entero. Ahora bien, si D es divisible por σ^2, lo serán t'^2 y t''^2, y, por consecuencia, σ estará contenido en t' y t'': de lo cual resulta que u es entero; y, si $4D \equiv \sigma^2 \pmod{4\sigma^2}$, será $(2t)^2 \equiv (\sigma u')^2 \pmod{4\sigma^2}$; y, por lo tanto, $2t' \equiv \sigma u'$, y tambien $2t'' \equiv \sigma u'' \pmod{2\sigma}$: de donde $2(t'u'' + u't'') \equiv 2\sigma u'u'' \equiv 0 \pmod{2\sigma}$; y u, asimismo, número entero.

Esta ley puede generalizarse y extenderse á un número cualquiera de soluciones (t', u'), (t'', u''), (t''', u''') ..... y tendremos:

$$\frac{t' + u'\sqrt{D}}{\sigma} \cdot \frac{t'' + u''\sqrt{D}}{\sigma} \cdot \frac{t''' + u'''\sqrt{D}}{\sigma} \cdots = \frac{t + u\sqrt{D}}{\sigma}$$

representando siempre (t, u) una nueva solucion entera. Y, si admitimos además que todas aquellas soluciones constan de números positivos, los factores del primer miembro de esta ecuacion, compuesto de los *primeros*, correspondientes á cada una de dichas soluciones, serán quebrados impropios positivos; lo mismo sucederá con el primer factor de la solucion (t, u); y, por consecuencia, los números t y u serán tambien positivos.

Supongamos ahora idénticas á la mínima (T, U) todas las soluciones positivas (t', u'), (t'', u'') ..... etc.: entónces la última ecuacion se convierte en la siguiente:

$$\left(\frac{T + U\sqrt{D}}{\sigma}\right)^n = \frac{t_n + u_n\sqrt{D}}{\sigma}$$

en la cual representa n un entero positivo cualquiera, y (t_n, u_n) una nueva solucion positiva. Su primer miembro, como potencia de un quebrado impropio, aumentará de valor al paso que se aumente el de n, é irá tambien creciendo, en consecuencia, $t_n + u_n\sqrt{D}$; de modo que á diferentes valores de n corresponderán diferentes soluciones (t_n, u_n); y, como los números t_n, u_n crecen ó menguan simultáneamente, crecerán, ó menguarán, cuando lo verifique n.

Mas recíprocamente: todas las soluciones positivas (t, u) pueden deducirse de la última fórmula. En efecto, supongamos, por un momento que así no suceda, esto es: que el primer factor de una solucion positiva (t, u), no sea exactamente igual á una potencia del primer factor de la solucion mínima (T, U); entónces, como los dos factores son quebrados impropios, deberá estar el primero comprendido entre dos potencias sucesivas,

$$\left(\frac{T+U\sqrt{D}}{\sigma}\right)^n, \quad \left(\frac{T+U\sqrt{D}}{\sigma}\right)^{n+1}$$

del segundo, siendo n, por lo ménos, $=1$; ó, expresándolo algebráicamente, deberán verificarse las desigualdades:

$$\frac{t_n+u_n\sqrt{D}}{\sigma} < \frac{t+u\sqrt{D}}{\sigma} < \frac{t_n+u_n\sqrt{D}}{\sigma}\cdot\frac{T+U\sqrt{D}}{\sigma};$$

ó bien, teniendo presente que

$$\frac{t_n+u_n\sqrt{D}}{\sigma}\cdot\frac{t_n-u_n\sqrt{D}}{\sigma}=1,$$

estas otras:

$$1 < \frac{t+u\sqrt{D}}{\sigma}\cdot\frac{t_n-u_n\sqrt{D}}{\sigma} < \frac{T+U\sqrt{D}}{\sigma}$$

de las cuales, haciendo

$$\frac{t+u\sqrt{D}}{\sigma}\cdot\frac{t_n-u_n\sqrt{D}}{\sigma}=\frac{t'+u'\sqrt{D}}{\sigma},$$

se deduciria que podia existir una solucion (t', u') formada por dos números t', u', menores que los constituyentes T, U, de la solucion mínima; y esto es absurdo.

La fórmula en cuestion, por consecuencia, es la expresion abreviada de todas las soluciones (t, u), compuestas de dos enteros positivos. Desarrollándola por la fórmula del binomio, y separando luego la parte racional de la irracional, se obtienen las dos siguientes:

$$\frac{t_n}{\sigma}=\frac{1}{\sigma^n}\left\{T^n+\frac{n(n-1)}{1.2}T^{n-2}U^2D+\ldots\ldots-\right\}$$

$$\frac{u_n}{\sigma}=\frac{1}{\sigma^n}\left\{\frac{n}{1}T^{n-1}U+\frac{n(n-1)(n-2)}{1.2.3}T^{n-3}U^3D+\ldots\ldots\right\}$$

que nos sirven para calcular todas las soluciones (t_n, u_n), mediante la mínima (T, U), dando á n sucesivamente los valores enteros y positivos de la série natural.

Mas por otra parte tenemos:

$$\frac{t_n-u_n\sqrt{D}}{\sigma}=\left(\frac{T-U\sqrt{D}}{\sigma}\right)^n=\left(\frac{T+U\sqrt{D}}{\sigma}\right)^{-n}.$$

Y esto prueba que, por la fórmula primera

$$\frac{t_n+u_n\sqrt{D}}{\sigma}=\left(\frac{T+U\sqrt{D}}{\sigma}\right)^n.$$

pueden calcularse todas las soluciones (t_n, u_n), en las que t_n sea positivo, atribuyendo á n todos los valores enteros, positivos y negativos, con tal que convengamos en establecer las igualdades $u_{-n} = -u_n$, $t_{-n} = -t_n$. Como además para $n = 0$, resultan $t_0 = +\sigma$, $u_0 = 0$, conclúyese que todas las soluciones (t, u), sin excepcion, de la ecuacion de Pell, pueden compendiarse en la fórmula

$$\frac{t + u\sqrt{D}}{\sigma} = \pm\left(\frac{T + U\sqrt{D}}{\sigma}\right)^n,$$

tomando siempre los dos signos para cada valor entero del exponente n. Y que, de esta manera, no queda fuera de dicha fórmula solucion ninguna, ni se obtiene más de una vez cada una de ellas, se colige inmediatamente reparando que entre las cuatro soluciones posibles,

$$(t, u),\ (t, -u),\ (-t, u),\ (-t, -u),$$

cuando no sea $u = 0$, existe una sola, constituida por dos números positivos.

Con esto queda por completo resuelto el segundo problema fundamental de las equivalencias para las formas con determinante *positiva;* pues por la resolucion completa de la ecuacion indeterminada $t^2 - Du^2 = \sigma^2$ se hallan desde luego todas las trasformaciones de una forma en sí misma; y todas las trasformaciones, por consecuencia, de una forma en otra equivalente, mediante una sola, conocida, de tales sustituciones (140) y (141). Y el problema de la construccion ó representacion de los números por formas con determinante positiva puede considerarse (139) asimismo como resuelto (*).

(*) Más pormenores sobre la ecuacion de Pell, y la representacion de los números por formas con determinante positiva encontrará el lector en el tomo 1.º de las obras de *Gauss*, pág. 192 y siguientes; como tambien la doctrina referente á las formas con determinante cuadrada y con determinante igual á cero, omitida en la presente.

Reduccion á la forma pelliana de la ecuacion general, binaria, de segundo grado.

—

La forma general de una ecuacion binaria de segundo grado es la siguiente:

$$a x^2 + b x y + c y^2 + d x + e y + f = 0 , \qquad (1)$$

en la cual los coeficientes enteros $a, b, c, \ldots\ldots$ pueden ser positivos y negativos, y tambien cero.

Multiplicando esta ecuacion por $4a$ resulta esta otra:

$$4a^2 x^2 + 4ab x y + 4ac y^2 + 4ad x + 4ae y + 4af = 0;$$

y de ésta, sumando con sus dos miembros la expresion $b^2 y^2 + 2bdy + d^2$, la que sigue:

$$(2ax + by + d)^2 = (by + d)^2 - 4a(cy^2 + ey + f)$$

de donde:

$$2ax + by + d = \sqrt{\{(by + d)^2 - 4a(cy^2 + ey + f)\}}$$

ó bien:

$$2ax + by + d = \sqrt{\{(b^2 - 4ac)y^2 + (2bd - 4ac)y + d^2 - 4af\}}.$$

Establezcamos ahora las igualdades:

$$2ax + by + d = u$$

$$b^2 - 4ac = A$$

$$2bd - 4ac = 2g$$

$$d^2 - 4af = h.$$

Con tales suposiciones la ecuacion anterior se convierte en

$$Ay^2 + 2gy + h = u^2$$

de la cual, multiplicándola por A, resultan sucesivamente:

$$A^2y^2 + 2Agy + Ah = Au^2$$

$$A^2y^2 + 2Agy + g^2 = Au^2 - Ah + g^2$$

$$(Ay + g)^2 = A(u^2 - h) + g^2$$

$$(Ay + g)^2 - Au^2 = g^2 - Ah.$$

Y haciendo:

$$Ay + g = t, \quad g^2 - Ah = B$$

se obtiene finalmente la forma:

$$t^2 - Au^2 = B. \qquad (2)$$

Hallados t y u, los valores de x é y se deducirán de las fórmulas:

$$y = \frac{t - g}{A}, \quad x = \frac{u - d - b\,y}{2\,a} = \frac{(u - d)\,A - b\,(t - g)}{2\,A\,a}.$$

Puesto que las variables t y u entran elevadas al cuadrado en la ecuacion resultante (2), podemos atribuirles indiferentemente valores positivos ó negativos en los fórmulas para x é y; y, si no se exije más que sean racionales las soluciones de la ecuacion propuesta (1), sólo valores de esta misma especie deberemos obtener de la convertida (2); pero, si hubieran de ser enteros los valores de las incógnitas x é y, es evidente que sólo podríamos introducir en las fórmulas para estas variables los valores convenientes de t y u para que de ellos resultaran los enteros que para x é y se piden; y entónces siempre seria más complicado el problema, y aún imposible muchas veces.

Ejemplo. Convertir la ecuacion

$$3x^2 + 8xy - 3y^2 + 2x - 5y = 110$$

en otra de la forma

$$t^2 - A\,u^2 = B.$$

Cotejando esta ecuacion particular con la general (1) resulta:

$$a = 3,\ b = 8,\ c = -3,\ d = 2,\ e = -5,\ f = -110:$$

y, por consecuencia:

$$b\,d - 2\,a\,e = g = 46$$

$$d^2 - A\,f = h = 1324$$

$$b^2 - A\,c = A = 100$$

$$g^2 - A\,h = B = -130284,$$

y, al fin, la ecuacion que se busca será:

$$t^2 - 100\,u^2 = -130284.$$

Con estas brevísimas consideraciones se corrobora la importancia, ya bien patente en la representacion de los números, de la ecuacion al parecer particular y sencilla que llamamos *pelliana;* pero todavía ha de manifestarse más su trascendencia en las investigaciones más profundas que todas las anteriores, del capítulo siguiente.

CAPITULO VII.

Del número de clases en que pueden distribuirse las formas cuadráticas, binarias, con una determinante conocida.

En el artículo (138) dijimos que todas las formas, pertenecientes á una misma determinante D, podian distribuirse en *clases;* y que, eligiendo un indivíduo de cada una de todas estas clases, se constituia un sistema completo S, de formas no equivalentes, para la expresada determinante. El número de formas, ó individuos contenidos en cada una de tales clases, no tiene límite; pero el número de representantes de cada una de ellas, ó lo que es igual, el conjunto de los términos de un sistema completo de formas no equivalentes, ó bien, el *número de clases de formas,* para una determinante dada, demostramos que era *finito:* ya fuese esta determinante negativa (147), ya fuera positiva (152). Determinar este número finito de clases de formas, para una determinante conocida, es el problema de que vamos á tratar ahora: iniciado en sus fundamentos por Gauss, y resuelto satisfactoriamente por Lejeune-Dirichlet con el auxilio poderoso del Cálculo infinitesimal.

Conjunto de los números susceptibles de ser representados por un sistema completo de formas primitivas.—Grupos de construcciones.

Como se indica en el epígrafe, nos concretamos en la cuestion presente á las formas *primitivas de primera y segunda especie* (140); y además, tratándose de las determinantes *negativas*, á las formas llamadas *positivas* (143).

Consideremos, pues, constituido un sistema completo S, de formas primitivas de especie σ, y comencemos por definir, ó caracterizar precisamente, los números en su totalidad que pueden ser construidos por las mismas.

Estos números, en lugar de designarlos por m como anteriormente, los expresaremos por σm, para comprender así los dos casos, referentes á sus formas representativas; en atencion á que por las primitivas de segunda especie sólo pueden ser representados números pares. Y entre tales números, σm, sólo estudiaremos aquéllos, en que m *sea positivo, impar y primo con la determinante* D. Todavía otra limitacion: las construcciones que emplearemos serán siempre las *propias;* esto es, aquéllas en que los números constructores x é y, sean primos relativos.

Esto sentado, para determinar el carácter de los números m, recordaremos que la determinante D, de toda forma representativa de un número σm, debe ser resto cuadrático de este número; ó bien que, si cualquier número σm es construido por una forma con la determinante D, la congruencia

$$z^2 \equiv D \,(\text{mod. } \sigma m)$$

será posible. Esto exige que todos los factores primos f, del número impar m, satisfagan á la condicion

$$\left(\frac{D}{f}\right) = 1.$$

Y recíprocamente: si el número m contiene solamente factores que satisfagan á esta condicion, y su conjunto es μ (sin exceptuar el caso de $\mu = 0$), la determinante D será resto cuadrático de m, y, por consecuencia, de σm, y la anterior congruencia comprenderá 2^{μ} raices incongruentes (139).

Designando por n una representante de tales raices, podremos establecer la igualdad $n^2 - D = \sigma^2 m l$, en la cual representará l un entero; porque, áun en el caso de ser $\sigma = 2$, y, por lo tanto, $D \equiv 1 \pmod 4$ (140), n será impar, y $n^2 - D$, de consiguiente, divisible por $\sigma^2 = 4$. La forma $(\sigma m, n, \sigma l)$, entónces, como m es primo con $2D$, será primitiva, de la especie σ, con la determinante D, y equivalente, por consecuencia, á una sola de las formas contenidas en el sistema S: luego, si (a, b, c) es esta forma, las construcciones (x, y) por la misma del número σm, serán exclusivamente las pertenecientes á la raiz individual n, de la congruencia mencionada; y tantas diferentes entre sí, como trasformaciones $\begin{pmatrix} x, & \xi \\ y, & \eta \end{pmatrix}$ puedan existir de la forma (a, b, c) en la $(\sigma m, n, \sigma l)$, esto es: tantas como soluciones (t, u), admita la ecuacion indeterminada $t^2 - D u^2 = \sigma^2$ (141 y 158).

Al conjunto de todas las construcciones (x, y), del número σm, pertenecientes á una raiz determinada n, de la congruencia $z^2 \equiv D \pmod{\sigma m}$, le damos el nombre de *grupo* de construcciones; y con esta definicion diremos ya que á las 2^{μ} raices de la citada congruencia corresponden 2^{μ} grupos de construcciones del número σm por las formas del sistema S: comprendiendo cada grupo tantas construcciones cuantas soluciones admita la ecuacion $t^2 - D u^2 = \sigma^2$.

En conclusion: el sistema de los números m se halla enteramente caracterizado por las condiciones siguientes:

1.ª m *es positivo.*

2.ª m *es primo con* $2D$.

3.ª D *es resto cuadrático de* m.

162. — *Número de las construcciones expresadas.*

Acabamos de decir que las construcciones (x, y) del número σm, por la forma (a, b, c), de determinante D, se dividen en grupos; y cada grupo comprende tantas, como soluciones (t, u) admita la ecuacion $t^2 - Du^2 = \sigma^2$. Pero esta ecuacion tiene un número *finito* de soluciones cuando la determinante D es negativa; y un número *infinito*, por el contrario, cuando sea D positiva; resultando de aquí que, respecto de las determinantes negativas, podremos hallar inmediatamente el número de las construcciones mencionadas; mas para encontrar dicho número, respecto de las determinantes positivas, es indispensable convertirlo previamente en finito. Con esta distincion estudiemos ante todo minuciosamente las construcciones pertenecientes á un mismo grupo.

Determinantes negativas.—En este caso es finito el número de soluciones de la ecuacion de Pell: designémosle por $\varkappa$; y conservando para μ y f la significacion que antes les dimos, resultará que el número de grupos de construcciones será 2^{μ}, y el total de las mismas, por consecuencia:

$$\varkappa \cdot 2^{\mu}.$$

En esta expresion, como sabemos (142), es:

$$\varkappa = 2, \text{ en general.}$$

$$\varkappa = 4, \text{ cuando } D = -1.$$

$$\varkappa = 6, \text{ cuando } D = -3 \text{ y } \sigma = 2.$$

Determinantes positivas.—El número de los grupos de construcciones es ahora tambien el mismo, 2^{μ}, que antes; pero el de las construcciones contenidas en cada grupo es infinito; y es preciso convertirlo en

finito, segun indicamos, imponiendo nuevas cortapisas á los números constructores, á fin de aislar, en primer término, *una sola* construccion de las infinitas que á un grupo corresponden. Designemos, pues, por (x, y) la forma general de las construcciones del número σm, contenidas en el mismo grupo. Si (a, b, c) representa, como antes, la forma del sistema S, equivalente á la $(\sigma m, n, \sigma l)$, y $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ una trasformacion, determinada, de la primera en la segunda, componiendo por la fórmula

$$\begin{pmatrix} \lambda, & \mu \\ \nu, & \rho \end{pmatrix} \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} = \begin{pmatrix} \lambda\alpha + \mu\gamma, & \lambda\beta + \mu\delta \\ \nu\alpha + \rho\gamma, & \nu\beta + \rho\delta \end{pmatrix},$$

la sustitucion dada, con cada una de las trasformaciones $\begin{pmatrix} \lambda, & \mu \\ \nu, & \rho \end{pmatrix}$ de la forma (a, b, c) en sí misma, se obtendrán todas las demás que convierten esta forma en su equivalente $(\sigma m, n, \sigma l)$. Pero, al aplicar esta fórmula sucesivamente á cada una de las sustituciones $\begin{pmatrix} \lambda, & \mu \\ \nu, & \rho \end{pmatrix}$, vamos hallando tambien todas las construcciones, realmente distintas, del número σm, pertenecientes á la raiz n: compuestas siempre en cada caso (139) de los coeficientes primero y tercero de la correspondiente sustitucion compuesta. Luego la forma general de todas las construcciones será la de los expresados coeficientes, á saber:

$$x = \lambda\alpha + \mu\gamma, \quad y = \nu\alpha + \rho\gamma;$$

y, como los coeficientes α, γ, de la sustitucion dada, forman ellos mismos una construccion (α, γ), resulta finalmente que todas las construcciones (x, y), pertenecientes á un grupo, pueden deducirse mediante las últimas fórmulas, de una cualquiera determinada (α, γ). Recordando ahora que, si (t, u) representa cualquiera de las soluciones de la ecuacion $t^2 - Du^2 = \sigma^2$, los valores de λ, μ, ν, ρ son:

$$\lambda = \frac{t - bu}{\sigma}, \quad \mu = -\frac{cu}{\sigma}, \quad \nu = \frac{au}{\sigma}, \quad \rho = \frac{t + bu}{\sigma},$$

las expresiones anteriores de x é y se convierten en las siguientes:

$$x = \alpha \frac{t}{\sigma} - (b\alpha + c\gamma)\frac{u}{\sigma}, \quad y = \gamma \frac{t}{\sigma} + (a\alpha + b\gamma)\frac{u}{\sigma}.$$

Multiplicando por a la ecuacion

$$a x^2 + 2 b x y + c y^2 = \sigma m.$$

se trasforma en la (134) siguiente:

$$\sigma a m = \{a x + (b + \sqrt{D}) y\} \times \{a x + (b - \sqrt{D}) y\};$$

é introduciendo los valores anteriores de x é y, que la satisfacen, en los factores irracionales que constituyen su segundo miembro, estos factores podrán ser expresados por las igualdades

$$a x + (b + \sqrt{D}) y = (a\alpha + (b + \sqrt{D})\gamma)\frac{t + u\sqrt{D}}{\sigma}$$

$$a x + (b - \sqrt{D}) y = (a\alpha + (b - \sqrt{D})\gamma)\frac{t - u\sqrt{D}}{\sigma}$$

de las que, designando por T, U los valores mínimos positivos de t, u, y haciendo por abreviar

$$\frac{T + U\sqrt{D}}{\sigma} = \theta,$$

se deducen estas otras (158):

$$a x + (b + \sqrt{D}) y = \pm (a\alpha + (b + \sqrt{D})\gamma)\theta^n$$

$$a x + (b - \sqrt{D}) y = \pm (a\alpha + (b - \sqrt{D})\gamma)\theta^{-n}$$

donde el exponente n puede representar un entero, positivo ó negativo, ó el cero, que patentizan ser cada uno de dichos factores una progresion geométrica.

Consideremos solamente la primera de estas igualdades; pues de ella se desprende sin esfuerzo cuanto se refiere á la otra. Su primer miembro, no considerado numéricamente, ó en absoluto, sino en el sentido algebráico, si k designa una cantidad real cualquiera, diferente de cero, puede mirarse como comprendido entre los límites k y $k\theta$, determinando convenientemente para ello el signo del segundo miembro y el exponente n. Esta determinacion puede efectuarse de un solo modo; en atencion á que, una vez elegido el signo $\pm$, de manera que la cantidad $\pm(a\alpha+(b+\sqrt{D})\gamma$ concuerde con k, entre este límite y el otro $k\theta$, existirá un solo término de la progresion geométrica, cuya expresion abreviada es dicho segundo miembro; con tal que, para evitar toda contingencia de indeterminacion, excluyamos ó pongamos fuera del alcance de la cantidad comprendida entre los límites mencionados uno cualquiera de estos: el θk, por ejemplo. Con estas condiciones, impuestas á la expresion $ax+(b+\sqrt{D})y$, podemos aislar completamente una construccion entre las infinitas (x, y) que al número σm corresponden. Pero resta saber todavía cómo habremos de determinar el valor de k de un modo conveniente para conseguir tal resultado.

Admitamos que la forma (a, b, c), representante de todas las de una clase de las comprendidas en el sistema S, tiene su primer coeficiente a positivo: condicion que se verifica en algunas formas reducidas de cada clase, fué exijida antes para las formas con determinante negativa, y no debemos olvidar en lo sucesivo para elegir las formas del sistema S, mencionado. Entónces, atendiendo á que sólo tratamos de construir números positivos, no hay inconveniente en atribuir á k el valor positivo de la raiz cuadrada de $\sigma a m$, y expresar, por lo tanto, las condiciones para aislar una sola de las construcciones (x, y), pertenecientes al mismo grupo, del número σm por la forma (a, b, c), del modo siguiente:

$$\sqrt{\sigma a m} \leq ax+(b+\sqrt{D})y < \theta\sqrt{\sigma a m},$$

donde se manifiesta la exclusion del segundo límite θk. Estas des-

igualdades, elevándolas al cuadrado, y teniendo en cuenta la expresion para $\sigma a m$, antes escrita, se convierten en estas otras:

$$a x + (b - \sqrt{D}) y \leqq a x + (b + \sqrt{D}) y < \theta^2 (a x + (b - \sqrt{D}) y).$$

De la primera, como $\sqrt{D}$ se considera positivo, resulta:

$$y \geqq 0;$$

y de la segunda, poniendo por θ su valor,

$$a x + b y > \frac{T}{U} y.$$

Y recíprocamente: de estas últimas condiciones de aislamiento

$$y \geqq 0, \quad a x + b y > \frac{T}{U} y,$$

retrocedemos á las anteriores sin obstáculo.

Pero hay más todavía: en virtud de las mismas se hace positivo el valor de la forma $(a, b, c) = a x^2 + 2 b x y + c y^2 = \sigma m;$ pues, agregando $\pm y \sqrt{D}$ á los dos miembros de esta segunda igualdad, se patentiza que los dos factores irracionales

$$a x + (b + \sqrt{D}) y, \quad a x + (b - \sqrt{D}) y,$$

son positivos; que su producto $\sigma a m$, por consecuencia, será positivo; y, como a lo es por eleccion, que lo mismo sucederá con σm, y, finalmente, con la forma (a, b, c). Esta circunstancia notable, tratándose de las formas con determinante negativa, no necesita prueba ninguna: se desprende naturalmente de que para estas determinantes sólo hemos estudiado las formas positivas.

Recapitulemos todo lo dicho, relativo á unas y otras determinantes:

Consideremos constituido un sistema completo S, de formas primitivas de la especie σ.

$$(a, b, c), \quad (a', b', c'), \quad (a'', b'', c'') \ldots\ldots:$$

para la determinante D. *En cada una de estas formas* (en la (a, b, c), por ejemplo, para podernos expresar claramente), *atribúyanse á las variables todos los pares de valores* (x, y) *que satisfagan á las condiciones:*

I. $\dfrac{ax^2 + 2bxy + cy^2}{\tau}$ *primo con* $2D$.

II. $y \geqq 0, \quad ax + by > \dfrac{T'}{U} y$, *cuando* D *sea positiva.*

III. x é y *primos entre sí.*

Con estas condiciones las formas S *representarán todos los números* τm *exclusivamente que satisfagan á las siguientes:*

1.ª m *positivo.*

2.ª m *primo con* $2D$.

3.ª D *resto cuadrático de* m.

Y el conjunto de las representaciones ó construcciones de cada número τm, *estará expresado por la forma*

$$\varkappa . 2^{\mu} :$$

en la cual μ *significa el número de factores primos, distintos,* f, *contenidos en* m; *y* $\varkappa$ *es una constante, independiente de* m, *que vale, segun hemos dicho:*

$\varkappa = 1$, *para las determinantes positivas* D;

$= 4$, *para* $D = -1$,

$= 6$, *para* $D = -3$ y $\tau = 2$,

$= 2$, *en todos los demás casos.*

163.—*Ecuacion fundamental.*

De los principios expuestos se concluye que el mismo sistema infinito de números σm, puede ser representado de dos maneras distintas: ó por el conjunto de los números primos f, de los cuales sea D resto cuadrático; ó sustituyendo todos los pares posibles de valores (x, y) en cada una de las formas S. Y este resultado de nuestras investigaciones anteriores, acerca de la equivalencia de las formas y la construccion de los números, constituye el principio fundamental de las venideras.

Desde luego es óbvio que, existiendo identidad entre los dos sistemas numéricos, expresados de los dos modos que hemos dicho, deberá existir tambien entre el conjunto de los números

$$\psi\left(\frac{ax^2+2bxy+cy^2}{\sigma}\right),\quad \psi\left(\frac{a'x^2+2b'xy+c'y^2}{\sigma}\right),\ \ldots\ldots$$

y el de los números $\psi(m)$; con tal que designemos por ψ una funcion determinada de cada uno de los números, en tales sistemas respectivamente comprendidos, y supongamos que el valor $\psi(m)$ de tal funcion, correspondiente á un indivíduo m, entra precisamente en el último sistema $\varkappa . 2^{\mu}$ veces. Calificando, pues, la funcion ψ, de modo que la *suma* de todos estos valores forme una série convergente, con independencia del órden de los mismos, la identidad antes indicada se expresará por la ecuacion

$$\Sigma\psi\left(\frac{ax^2+2bxy+cy^2}{\sigma}\right)+\Sigma\psi\left(\frac{a'x^2+2b'xy+c'y^2}{\sigma}\right)+\ldots\ldots=\varkappa\Sigma 2^{\mu}\psi(m),$$

que lleva el nombre de *fundamental*.

Su primer miembro contiene tantas sumas *principales* como formas (a, b, c), (a', b', c') ..... el sistema S; ó, en otros términos, tantas como

clases de formas existen para la determinante D. Y cada suma principal, como, por ejemplo, la

$$\Sigma \psi\left(\frac{a x^2 + 2 b x y + c y^2}{\sigma}\right).$$

es una doble série infinita, cuyos términos corresponden á todos los pares de valores (x, y), definidos por las condiciones I, II, III, del artículo último (modificadas naturalmente la I y la II cuando se refieran á la forma (a', b', c') en vez de á la (a, b, c), etc.)

En su segundo miembro existe un signo de suma tambien que se refiere á todos los números m, compuestos de los números primos f; y las letras μ y $\varkappa$ conservan la misma significacion que antes les dimos.

Por último, si definimos la funcion ψ por la relacion

$$\psi(z) = \frac{1}{z^s},$$

en la cual puede recibir s un valor cualquiera positivo, pero mayor que la unidad, las séries infinitas, de que hablamos poco más arriba, serán convergentes, como demostraremos luégo, y la ecuacion fundamental se convierte en la que sigue:

$$\Sigma \left(\frac{a x^2 + 2 b x y + c y^2}{\sigma}\right)^{-s} + \ldots\ldots = \varkappa \Sigma \frac{2^\mu}{m^s};$$

expresada, para no escribir tanto, por una sola suma principal.

164.—*Trasformacion del segundo miembro de esta ecuacion.*

Designemos por

$$f_1, f_2, f_3, \ldots\ldots$$

el conjunto de todos los números primos f, no contenidos en $2D$, y

de los cuales es D resto cuadrático; cualquiera de los números m, antes definidos, podrá ser expresado entónces, y de un solo modo, por la forma

$$f_1^{\prime\prime 1} \cdot f_2^{\prime\prime 2} \cdot f_3^{\prime\prime 3} \cdot \ldots$$

en la cual significan los exponentes $n_1, n_2, n_3 \ldots$ enteros positivos, ó cero.

Desenvolvamos la suma que figura en el segundo miembro de la ecuacion última en las correspondientes á cada uno de los factores primos f, del número m, y obtendremos las séries infinitas parciales:

$$1 + \frac{2}{f_1^s} + \frac{2}{f_1^{2s}} + \frac{2}{f_1^{3s}} + \ldots + \frac{2}{f_1^{n_1 s}} + \ldots$$

$$1 + \frac{2}{f_2^s} + \frac{2}{f_2^{2s}} + \frac{2}{f_2^{3s}} + \ldots + \frac{2}{f_2^{n_2 s}} + \ldots$$

$$1 + \frac{2}{f_3^s} + \frac{2}{f_3^{2s}} + \frac{2}{f_3^{3s}} + \ldots + \frac{2}{f_3^{n_3 s}} + \ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

El producto de un término cualquiera de la primera série, por uno cualquiera de la segunda, por otro de la tercera, etc., tiene evidentemente la forma general

$$\frac{2^\mu}{\left(f_1^{\prime\prime 1} \cdot f_2^{\prime\prime 2} \cdot f_3^{\prime\prime 3} \ldots \right)^s} = \frac{2^\mu}{m^s}$$

donde μ expresa el número de los factores primos (45) del número m.

Aplicando esta forma se obtienen los términos realmente distintos de la mencionada suma $\Sigma \frac{2^{\nu}}{m^s}$, que es, por lo tanto, igual en su totalidad al producto de todas las séries parciales anteriores. Considerando, pues, que cada una de éstas séries comprende una progresion geométrica infinita, cuya razon es $\frac{1}{f^s}$, y cuya suma, por lo tanto, es en general:

$$1+\frac{2}{f^s}+\frac{2}{f^{2s}}+\frac{2}{f^{3s}}+\ldots\ldots+\frac{2}{f^{ns}}+\ldots\ldots=$$

$$=1+\frac{2}{f^s}\cdot\frac{1}{1-\frac{1}{f^s}}=\frac{1+\frac{1}{f^s}}{1-\frac{1}{f^s}}$$

podremos escribir:

$$\Sigma\frac{2^{\nu}}{m^s}=\Pi\frac{1+\frac{1}{f^s}}{1-\frac{1}{f^s}}$$

refiriéndose el signo-producto Π, como es consiguiente, á todos los factores primos f, del número m.

El segundo miembro de esta última ecuacion puede á su vez modificarse en sentido más amplio del modo siguiente. Designemos por q *un número primo cualquiera, positivo, no contenido en* $2D$; será:

$$\Sigma\frac{2^{\nu}}{m^s}=\Pi\frac{1+\frac{1}{q^s}}{1-\left(\frac{D}{q}\right)\frac{1}{q^s}}\ :$$

puesto que siempre que el número q no pertenezca á los factores, f, no será D resto cuadrático suyo; el símbolo $\left(\frac{D}{q}\right)$ será la unidad negativa; y el factor correspondiente del producto se reducirá á $+1$. Multiplíquense por $(1-\frac{1}{q^s})$ los dos términos del quebrado bajo el signo II, y tendremos:

$$\frac{1-\frac{1}{q^{2s}}}{\left(1-\frac{1}{q^s}\right)\left(1-\left(\frac{D}{q}\right)\frac{1}{q^s}\right)} = \frac{\left(\frac{1}{1-\frac{1}{q^s}}\right)\left(\frac{1}{1-\left(\frac{D}{q}\right)\frac{1}{q^s}}\right)}{\left(\frac{1}{1-\frac{1}{q^{2s}}}\right)}$$

Y de este modo el producto infinito en cuestion podemos descomponerlo en tres, tambien infinitos, segun á continuacion se expresa:

$$\Sigma\frac{\mathfrak{D}^{\mu}}{m^s} = \frac{\Pi\frac{1}{1-\frac{1}{q^s}}\cdot\Pi\frac{1}{1-\left(\frac{D}{q}\right)\frac{1}{q^s}}}{\Pi\frac{1}{1-\frac{1}{q^{2s}}}}.$$

Cada uno de dichos tres productos se trasforma de nuevo en una série infinita; pues, efectuando la division, se halla fácilmente:

$$\frac{1}{1-\left(\frac{D}{q}\right)\frac{1}{q^s}} = 1+\left(\frac{D}{q}\right)\frac{1}{q^s}+\left(\frac{D}{q}\right)^2\frac{1}{q^{2s}}+\ldots.+$$

$$+\left(\frac{D}{q}\right)^r\frac{1}{q^{rs}}+\ldots.. = \Sigma\left(\frac{D}{q}\right)^r\frac{1}{q^{rs}}:$$

y, si sustituimos ahora por q todos los números primos $q_1, q_2, q_3, \ldots\ldots$ no contenidos en $2D$, el producto de todos los factores correspondientes á estos números primos será igual á la suma de todos los términos de la forma general, arriba para un solo número primo q indicada:

$$\left(\frac{D}{q_1}\right)^{r_1}\left(\frac{D}{q_2}\right)^{r_2}\left(\frac{D}{q_3}\right)^{r_3}\ldots\ldots\ \frac{1}{\left(q_1^{r_1}\ q_2^{r_2}\ q_3^{r_3}\ldots\ldots\right)^s}$$

en la cual representan los exponentes $r_1, r_2, r_3, \ldots\ldots$ todos los números enteros, positivos, y tambien el cero. Pero, con tales condiciones, la forma

$$q_1^{r_1}\ q_2^{r_2}\ q_3^{r_3}\ldots\ldots = n,$$

comprende evidentemente todos los *números enteros positivos* n, *primos con* $2D$, correspondiendo á uno solo de ellos cada sistema determinado de los exponentes r; y, por otra parte, conforme con la significacion del símbolo de *Jacobi* (118), se halla:

$$\left(\frac{D}{q_1}\right)^{r_1}\left(\frac{D}{q_2}\right)^{r_2}\left(\frac{D}{q_3}\right)^{r_3}\ldots\ldots = \left(\frac{D}{q_1^{r_1}}\right)\left(\frac{D}{q_2^{r_2}}\right)\left(\frac{D}{q_3^{r_3}}\right)\ldots\ldots = \left(\frac{D}{n}\right),$$

luego efectivamente:

$$\Pi\ \frac{1}{1-\left(\frac{D}{q}\right)\frac{1}{q^s}} = \Sigma\left(\frac{D}{n}\right)\frac{1}{n^s},$$

refiriéndose el signo sumatorio del segundo miembro de esta igualdad á todos los números positivos n, primos con $2D$.

Procediendo del mismo modo con los otros productos, y multiplicando entre sí todos los desarrollos

$$\frac{1}{1-\frac{1}{q^s}} = 1 + \frac{1}{q^s} + \frac{1}{q^{2s}} + \ldots\ldots + \frac{1}{q^{rs}} + \ldots\ldots +$$

correspondientes á cada uno de los números determinados $q_1, q_2, q_3 \ldots\ldots$, se obtiene:

$$\Pi \frac{1}{1-\frac{1}{q^s}} = \Sigma \frac{1}{n^s} \quad \text{y, por tanto:} \quad \Pi \frac{1}{1-\frac{1}{q^{2s}}} = \Sigma \frac{1}{n^{2s}}.$$

De todo lo cual resulta la notable trasformacion que buscábamos:

$$\Sigma \frac{2^{\omega}}{n^s} = \frac{\Sigma \frac{1}{n^s} \times \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s}}{\Sigma \frac{1}{n^{2s}}}.$$

165.—*Modificacion de la ecuacion fundamental para que pueda ser tambien satisfecha por construcciones impropias.*

En un principio dijimos que las construcciones de un número por una forma, de las cuales íbamos á tratar, eran, mientras expresamente no se declarase lo contrario, las llamadas *propias*, esto es, aquellas en que los números constructores x, y, son primos relativos. Y con esta condicion dedujimos la ecuacion fundamental (163); que procuramos trasformar ahora de modo que comprenda tambien las construcciones *impropias*.

Multipliquemos para ello dicha ecuacion por la série

$$\Sigma \frac{1}{n^{2s}} = \Sigma n^{-2s},$$

y, teniendo en cuenta el último resultado del artículo precedente, obtendremos la siguiente:

$$\Sigma n^{-2s} \times \Sigma \left(\frac{a x^2 + 2 b x y + c y^2}{\sigma} \right)^{-s} = \varkappa \Sigma \frac{1}{n^s} \times \Sigma \left(\frac{D}{n} \right) \frac{1}{n^s}.$$

Efectuando la multiplicacion de las dos sumas, indicada en el primer miembro, el resultado

$$\Sigma \left(\frac{a n^2 x^2 + 2 b n^2 x y + c n^2 y^2}{\sigma} \right)^{-s},$$

es claramente una série triplemente infinita en la cual pueden recibir x é y todos los valores que satisfagan á las condiciones I, II y III, y n representa todos los números positivos y primos con $2D$.

Establezcamos ahora las igualdades

$$u x = x' \qquad u y = y':$$

la série triplemente infinita, anterior, se convertirá en la doblemente infinita

$$\Sigma \left(\frac{a x'^2 + 2 b x' y' + c y'^2}{\sigma} \right)^{-s}.$$

y la cuestion se reduce á averiguar solamente las condiciones á que deberán satisfacer los nuevos sumandos ó números constructores x' é y'. Estas condiciones se deducen sencillamente de las establecidas ya para x, y, n.

En efecto, x é y, dijimos, es necesario elegirlas de modo que la expresion

$$\frac{a x^2 + 2 b x y + c y^2}{\sigma}$$

adquiriera un valor primo con $2D$; y, como n es tambien primo con $2D$, en nada habrá que modificar la eleccion de x é y para que

$$\frac{a x'^2 + 2 b x' y' + c y'^2}{\sigma} = n^2 . \frac{a x^2 + 2 b x y + c y^2}{\sigma}$$

adquiera un valor tambien primo con $2D$.

Para el caso de una determinante positiva, sabemos ya que las condiciones II, de separacion ó aislamiento, á que deben estar sujetos los números x é y, eran:

$$y \geqq 0, \quad a x + b y > \frac{T}{U} y.$$

Pues, multiplicándolas por n, los nuevos números constructores x', y', deberán obedecer á estas otras, idénticas en el fondo á las anteriores:

$$y' \geqq 0, \quad a x' + b y' > \frac{T}{U} y'.$$

Y, por último, de la condicion impuesta á los números x é y, de ser primos relativos, se desprende únicamente, respecto del caso actual, que el máximo comun divisor n de los x' é y' sea primo con $2D$; pero tal condicion está ya comprendida en la primera que hemos considerado; porque, si x' é y' tuviesen un divisor comun, que no fuese primo con $2D$, el valor correspondiente de la expresión

$$\frac{a x'^2 + 2 b x' y' + c y'^2}{\sigma}$$

no podria ser tampoco primo con $2D$; y deberia, en consecuencia, desecharse.

Resulta, pues, que las nuevas variables x', y', sólo deben satisfacer á las condiciones antes establecidas, I y II (aunque convenientemente acentuadas), sobrando respecto de ellas la otra condicion III. Y recíprocamente: que cada par de valores, ó construccion (x', y'), puede de un solo modo ser producido por otro par (x, y), y un número n.

Suprimiendo para mayor comodidad los acentos, la ecuacion fundamental puede ser expresada como sigue:

$$\Sigma\left(\frac{a x^2 + 2 b x y + c y^2}{\sigma}\right)^{-s} + \ldots\ldots = \varkappa \Sigma \frac{1}{n^s} \times \Sigma\left(\frac{D}{n}\right)\frac{1}{n^s},$$

donde las variables, ó letras sumandas, correspondientes á la suma principal, relativa á la forma (a, b, c), deben sólo satisfacer á las condiciones:

I. El valor de $\dfrac{a x^2 + 2 b x y + c y^2}{\sigma}$ debe ser primo con $2D$.

II. Para el caso de las determinantes positivas deben ser:

$$y \geq 0. \quad a x + b y > \frac{T}{U} y,$$

conservando T y U la significacion que desde luego les atribuimos.

166.—*Consecuencias interesantes de la doctrina precedente.*

a-) De la última ecuacion se deducen algunas, que completan la teoría de la construccion de los números, y merecen que por breve rato interrumpamos el discurso de nuestras principales investigaciones.

Despues de acentuar la letra n en las dos séries,

$$\Sigma \frac{1}{n'^s} \qquad \text{y} \qquad \Sigma\left(\frac{D}{n''}\right)\frac{1}{n''}$$

para distinguirlas entre sí, multipliquémoslas una por otra; el producto resultante

$$\Sigma\left(\frac{D}{n''}\right)\frac{1}{(n'\,n'')^s}$$

representará una série doblemente infinita en la que, tanto n' como n'' pueden recibir todos los valores de n: esto es, los de todos los números positivos y primos con $2D$. Pero entre estos números se halla evidentemente cada producto $n'\,n''$: luego, reuniendo siempre en uno solo todos los términos de la série ó suma doblemente infinita, anterior, en los cuales tenga el producto $n'\,n''$ el mismo valor n, dicha doble suma podrá expresarse bajo la forma

$$\Sigma\frac{\tau}{n^s}.$$

de una série simplemente infinita nada más, en la que, si δ designa cualquiera de los divisores del número n, es evidentemente:

$$\tau=\Sigma\left(\frac{D}{\delta}\right).$$

Trasformado así el segundo miembro, multipliquemos los dos de la ecuacion fundamental por σ^s, y tomará la forma

$$\Sigma\frac{1}{(a\,x^2+2\,b\,x\,y+c\,y^2)^s}+\ldots\ldots=\Sigma\frac{\varkappa\,\tau}{(\sigma\,n)^s};$$

y, reuniendo ahora tambien en uno solo todos los términos de igual valor comprendidos en las dobles sumas del primer miembro, la siguiente:

$$\Sigma\frac{\lambda}{\nu^s}=\Sigma\frac{\varkappa\,\tau}{(\sigma\,n)^s}.$$

significando ν todos los números representados por las formas (a, b, c), ...

del sistema S, y λ el conjunto de las construcciones diferentes para cada uno de ellos. Bueno es que notemos que, al hablar aquí de construcciones, comprendemos tanto las propias como las impropias; en atencion que los números constructores $x, y,$ tienen que satisfacer solamente á las condiciones I y II, del último artículo, pero no á la de ser además primos entre sí, como antes exijimos.

Hagamos ahora una digresion indispensable. Admitamos que para todo valor positivo del exponente s, que traspase cierto límite, se verifica la igualdad

$$\frac{\alpha}{a^s} + \frac{\beta}{b^s} + \frac{\gamma}{c^s} + \ldots\ldots = \frac{\alpha'}{a'^s} + \frac{\beta'}{b'^s} + \frac{\gamma'}{c'^s} + \ldots\ldots$$

donde, tanto las letras $a, b, c, \ldots\ldots$ como las $a', b', c',$ representen valores numéricos positivos y sucesivamente crecientes, y los coeficientes $\alpha, \beta, \gamma, \ldots\ldots$ y $\alpha', \beta', \gamma', \ldots\ldots$ valores diferentes de cero. Con tales condiciones, las dos séries que constituyen los dos miembros de dicha igualdad son enteramente idénticas, ó, lo que es igual, se verifican tambien las igualdades:

$$a = a', \quad b = b', \quad c = c', \ldots\ldots$$

$$\alpha = \alpha', \quad \beta = \beta', \quad \gamma = \gamma' \ldots\ldots$$

Para demostrarlo, admitamos por un momento que sea $a \leqq a'$; y multipliquemos por a^s los dos miembros de la igualdad propuesta que se convertirá de este modo en la siguiente:

$$\alpha + \beta\left(\frac{a}{b}\right)^s + \gamma\left(\frac{a}{c}\right)^s + \ldots\ldots = \alpha'\left(\frac{a}{a'}\right)^s + \beta'\left(\frac{a}{b'}\right)^s + \gamma'\left(\frac{a}{c'}\right)^s + \ldots\ldots$$

Como los quebrados

$$\frac{a}{b}, \quad \frac{a}{c}\ldots\ldots, \text{ y los } \frac{a}{a'}, \quad \frac{a}{b'} \ldots\ldots$$

son propios, que van disminuyendo, y ambas séries convergen, el primer

miembro de la última ecuacion, creciendo s indefinidamente, se aproxima al límite α, y el segundo al límite α', ó al límite 0, segun que sea $a = a'$, ó $a > a'$. Mas, siendo iguales las dos séries en cuestion, deben necesariamente aproximarse al mismo límite; y, puesto que α es diferente de cero, deberá ser $a = a'$; y tambien, por consecuencia, $\alpha = \alpha'$. Demostrada así la identidad de los dos primeros términos de las dos séries ó miembros de la ecuacion supuesta al principio, fácil séria probar que los dos segundos, y todos los demás, son tambien idénticos; porque, suprimiendo los dos primeros, en la ecuacion resultante

$$\frac{\beta}{b^s} + \frac{\gamma}{c^s} + \ldots = \frac{\beta'}{b'^s} + \frac{\gamma'}{c'^s} + \ldots$$

se probaria, por el mismo procedimiento, que $b = b'$, y por tanto $\beta = \beta'$; y así podríamos continuar hasta la demostracion completa de las identidades relativas á todos los términos.

Aplicando este resultado á la ecuacion fundamental, en la forma última que le dimos, se advierte que todo número σn, al cual corresponda un valor de τ, diferente de cero, será uno de los designados por ν, esto es, uno de los representados por las formas S; y, por el contrario, que si $\tau = 0$, el número σn no podrá contarse entre los ν, ó, lo que es igual, no podrá ser construido por las formas S; siendo, en el primer caso, igual á $\varkappa\tau$ el número λ de las construcciones diferentes de cada uno de los números $\sigma n = \nu$. De lo cual se desprende que

El número de todas las construcciones de un número σn por las formas S, es siempre igual á

$$\varkappa\tau = \varkappa \Sigma \left(\frac{D}{\delta}\right)$$

conservando δ la significacion que antes le dimos.

En esta conclusion general se hallan comprendidos algunos casos particulares que conviene estudiar.

1.° Sea $D = -1$; y, por consecuencia, $\sigma = 1$. En el sistema S habrá entónces una sola forma cuya representante definida es $(1, 0, 1)$; el sistema de los números σn será el de los números impares positivos n; y, como $\varkappa = 4$, resulta que:

El número de todas las construcciones de un número impar positivo, cualquiera, n, por la forma $(1, 0, 1) = x^2 + y^2$ es igual á

$$4 \Sigma (-1)^{\frac{1}{2}(\delta-1)} = 4 (M - N):$$

esto es: al cuádruplo de la diferencia entre el número M, de sus divisores ó de la forma $4h + 1$, y el número N de sus divisores de la forma $4h + 3$.

Aquí no existe para los números constructores x, y, ninguna limitacion; cada ocho construcciones distintas (148) producen una sola descomposicion en dos cuadrados de los números n, excepto cuando uno de los constructores sea cero; que entónces producen una descomposicion cuatro construcciones solamente, y n debe asimismo ser un cuadrado. De lo cual resulta que el número de las descomposiciones diferentes será $\frac{1}{2}(M - N + 1)$, ó $\frac{1}{2}(M - N)$, segun que el número descomponendo sea un cuadrado, ó no lo sea. Asi, por ejemplo:

$25 = 0^2 + 5^2 = 3^2 + 4^2$; pues $M=3$, $N=0$; y $\frac{1}{2}(M-N+1)=2$.

$45 = 3^2 + 6^2$: sus divisores: 1, 3, 9, 5, 15, 45; $M=4$, $N=2$.

$49 = 0^2 + 7^2$: » 1, 7, 49; $M=2$, $N=1$.

$65 = 1^2 + 8^2 = 4^2 + 7^2$: » 1, 5, 13, 65; $M=4$, $N=0$.

Si n fuese un número primo, tambien se deduciria de lo anterior que podria ser descompuesto en dos cuadrados de un solo modo, ó de ninguno, segun afectara la forma $4h+1$, ó la $4h+3$: como ya sabíamos (148).

2.° Para la determinante positiva $D=2$ sólo existen las dos formas reducidas equivalentes, $(1, 1, -1)$ y $(-1, 1, 1)$, y, de consiguiente, una sola clase, por cuya representante podremos tomar tambien (148) la forma $(1, 0, -2) = x^2 - 2y^2$.

Como la solucion mínima de la ecuacion $t^2 - 2u^2 = 1$, es $T = 3$, $U = 2$, los números constructores deberán satisfacer solamente á las condiciones

$$y \geqq 0, \quad 2x > 3y.$$

Pero tenemos por otra parte (114)

$$\left(\frac{2}{\delta}\right) = (-1)^{\frac{1}{8}(\delta-1)} = +1 \text{ ó } -1,$$

segun $\delta = 8h \pm 1$, ú $8h \pm 5$. Luego:

El número de todas las construcciones (x, y), *sujetas á las condiciones expresadas, de un número impar, positivo,* n, *por la forma* $x^2 - 2y^2$, *es igual á la diferencia entre el número de los divisores de* n, *cuya forma sea* $8h \pm 1$, *y el de los otros divisores.*

b-) No ya precisamente á la teoría de la construccion de los números, sino al *Análisis* en general, pertenecen otros corolarios de la ecuacion fundamental de que vamos á tratar seguidamente.

Acabamos de demostrar que los números σn se obtienen mediante la forma (a, b, c) del sistema S, sustituyendo en ella todos los pares (x, y) de valores numéricos que cumplan con las condiciones I y II del artículo (162), representando además

$$\varkappa\tau = \varkappa\Sigma\left(\frac{D}{\delta}\right)$$

el número de las construcciones de σn por dicha forma (a, b, c), con tal que δ recorra sucesivamente todos los divisores de n. Si por ψ designamos una funcion determinada, cada valor de esta funcion referida á cada uno de los números $ax^2 + 2bxy + cy^2$, esto es, cada valor de $\psi(\sigma n)$ podremos así producirlo tantas veces como expresa $\varkappa\tau$: de donde nuevamente se desprende la igualdad

$$\Sigma\psi(ax^2 + 2bxy + cy^2) + \ldots\ldots = \varkappa\Sigma\tau\psi(\sigma n):$$

para cuya verificacion es indispensable que se escoja ó defina la funcion

ψ, de modo que las sumas de las séries infinitas á que afecta, puedan ser determinadas prescindiendo del órden de sus términos. Así acontecerá ciertamente, si dicha funcion ψ se define por la relacion

$$\psi(z) = q^z,$$

en la cual representa q una cantidad real, ó compleja cuyo módulo sea un quebrado propio. Aplicando esta relacion, determinativa de la funcion ψ, á la ecuacion anterior, resulta la siguiente:

$$\Sigma q^{ax^2+2bxy+cy^2+\ldots\ldots} = \varkappa \Sigma \tau q^{\sigma u};$$

que, recordando la significacion de $\tau = \Sigma\left(\frac{D}{\delta}\right)$, y haciendo $n = n'\delta$, podrá escribirse de este otro modo:

$$\Sigma q^{ax^2+2bxy+cy^2+\ldots\ldots} = \varkappa \Sigma\left(\frac{D}{\delta}\right) q^{\sigma n'\delta}$$

en cuyo segundo miembro existe una doble suma, referida á las letras n' y δ que pueden recibir todos los valores numéricos n.

Examinemos ahora algunos casos particulares, en esta última ecuacion general comprendidos.

1.° Sea $D = -1$, y, por lo tanto, $\sigma = 1$. En tál supuesto, comprende el primer miembro una sola doble suma que es, tomando la forma $(1, 0, 1)$ para representar la clase correspondiente á la determinante dada,

$$\Sigma q^{x^2+y^2}.$$

En esta doble suma pueden las variables x é y recibir todos los pares de valores que hagan impar la expresion $x^2 + y^2$; y para esto es necesario que uno de los números x é y sea par, y el otro impar; mas, como en cada combinacion posible se pueden permutar entre sí tales números, no hay inconveniente en fijar que el x represente sola-

mente los impares, y los pares el y; y entónces deberemos multiplicar por 2 la doble suma en cuestion, ya restringida, que se convertirá en la

$$2\Sigma q^{x^2+y^2} = 2\Sigma q^{x^2} \times q^{y^2} = 2\Sigma q^{x^2} \times \Sigma q^{y^2},$$

donde la x puede tomar todos los valores impares, positivos y negativos; y la y todos los pares, positivos y negativos, y el cero. Y, si todavía concretamos los valores que puede recibir x á los impares positivos solamente, y los de y tambien á los pares positivos, el último producto se expresará del modo siguiente:

$$4\Sigma q^{x^2} \times (1 + 2\Sigma q^{y^2}).$$

Respecto del segundo miembro de la ecuacion general, diremos que en el caso actual es $\varkappa = 4$, y que en él existe, por consecuencia, la doble suma

$$4\Sigma\left(\frac{-1}{\delta}\right) q^{n'\delta} = 4\Sigma(-1)^{\frac{1}{2}(\delta-1)} q^{n'\delta},$$

en la que pueden recibir n' y δ todos los valores impares, positivos. Efectuando la suma respecto de n', se halla:

$$\Sigma q^{n'\delta} = q^{\delta} + q^{3\delta} + q^{5\delta} + \ldots = \frac{q^{\delta}}{1 - q^{2\delta}}$$

y, con esto, la expresion anterior toma la forma:

$$4\Sigma(-1)^{\frac{1}{2}(\delta-1)} \frac{q^{\delta}}{1 - q^{2\delta}}.$$

Y la ecuacion general, finalmente, la que sigue:

$$\Sigma q^{x^2} \times (1 + 2\Sigma q^{y^2}) = \Sigma (-1)^{\frac{1}{2}(\delta-1)} \frac{q^{\delta}}{1-q^{2\delta}}.$$

Para desarrollar esta ecuacion simbólica atribuiremos, en conformidad con lo dicho, á las x todos los valores impares, á la y los pares, y á la δ tambien los impares, de la série natural: y así se obtiene la muy notable

$$(q + q^9 + q^{25} + q^{49} + \ldots\ldots)\,(1 + 2q^4 + 2q^{16} + 2q^{36} + 2q^{64} + \ldots\ldots) =$$

$$= \frac{q}{1-q^2} - \frac{q^3}{1-q^6} + \frac{q^5}{1-q^{10}} - \frac{q^7}{1-q^{14}} + \ldots\ldots,$$

que pertenece á las determinantes negativas, y juega tambien en la Teoría de las funciones elípticas.

No son tan sencillas las ecuaciones referentes á las determinantes positivas; pues las variables x é y, en su primer miembro, deben someterse además á las condiciones II (162). Así, por ejemplo, para la determinante $D = 2$, en cuyo caso $\sigma = 1$, $\varkappa = 1$, hallamos de un modo semejante al explicado, la ecuacion

$$\Sigma q^{x^2-2y^2} = \Sigma \left(\frac{2}{\delta}\right) q^{\frac{1}{8}(\delta^2-1)} = \frac{q}{1-q^2} - \frac{q^3}{1-q^6} - \frac{q^5}{1-q^{10}} + \frac{q^7}{1-q^{14}} + \ldots\ldots$$

en la que pueden ser sustituidas las variables (x, y) por todos los pares de valores que satisfagan á las condiciones $y \geqq 0$, $2x > 3y$; y á la de ser además impar la expresion $x^2 - 2y^2$, y la variable x, por consecuencia.

167.—*Restricciones que deben imponerse á las formas representantes de las clases.*

—

Despues de la digresion anterior, continuemos ahora el exámen de nuestro asunto principal, por corto rato interrumpido, reanudando nuestro estudio con algunas indicaciones que enlacen de un modo manifiesto lo precedente con lo subsiguiente. En el artículo (165) quedó ya trasformada la ecuacion fundamental poco antes instituida. Esta ecuacion era:

$$\Sigma\left(\frac{a x^2 + 2 b x y + c y^2}{\sigma}\right)^{-s} + \ldots\ldots \quad \varkappa \Sigma \frac{1}{n^s} \times \Sigma\left(\frac{D}{n}\right) \frac{1}{n^s}.$$

Échase de ver en seguida la dificultad insuperable de efectuar las sumas indicadas en su primer miembro, respecto de cualesquiera valores de s, superiores á la unidad: sumas que entónces no tendrian límite, ni serian, por consecuencia, susceptibles de figurar, como elementos numéricos determinados, en ningun cálculo concreto, como lo es el de que ahora se trata. Pero, si establecemos que los valores de s vayan disminuyendo sin cesar y acercándose al límite 1, en cuyo supuesto irá creciendo simultáneamente, sin límite superior por grande que nos le figuremos, cada una de las sumas llamadas principales, que constituyen el mencionado primer miembro de la ecuacion fundamental, se advierte, pensando un poco más en el asunto, que el producto de una cualquiera de dichas sumas principales por la diferencia $(s-1)$, que tiene, segun lo establecido, por límite el *cero*, converge tambien hácia un límite finito y determinado L, dependiente sólo de la determinante comun, D, á todas las formas del sistema. Y claro es que, si tal producto, que pudiéramos llamar parcial, se aproxima al límite L, el producto total, esto es, el de todas las sumas principales, ó de todo el primer miembro de la ecuacion fundamental, por el mismo factor $(s-1)$, tendrá por límite el producto $h\,L$, designando por h el número de las sumas principales, ó lo que es igual, el número de formas

distintas (a, b, c), contenidas en el sistema S, cuya expresion analítica, concreta, buscamos principalmente. Esta expresion definida del número h, primer objeto de nuestro estudio en este Capítulo, como ya declaramos, exije para su indagacion que el segundo miembro de la ecuacion fundamental, multiplicado por el mismo factor $(s-1)$, que ha definido el primero, se acerque tambien á un límite fijo. Este valor, límite, sabemos hallarlo directamente; pero, antes de exponer el procedimiento para ello, y como preliminares indispensables al mismo fin, debemos concretar las condiciones de las formas que hayamos de elegir para representantes de sus clases respectivas en el sistema S.

Con este propósito vamos desde luego á trasformar la condicion I (162), impuesta á las variables x, y, de modo que exprese claramente el carácter de los números, ó del sistema de los pares de valores (x, y), segun decimos, que la satisfagan. Y de resultas veremos despues que la forma (a, b, c), representante de una clase, puede siempre elegirse con la propiedad de que el cociente $a : \sigma$ no sea positivo solamente, como ya se exigió antes, sino además *primo* con $2D$.

Sea, pues,

$$(a, b, c) = \sigma (A x^2 + B x y + C y^2) = \sigma F$$

una forma cualquiera de divisor σ, y r un número primo; no hay obstáculo en atribuir á las dos variables x é y valores convenientes para que el resultante de F no sea divisible por r; pues, en la suposicion de que uno de los dos coeficientes, A ó C de F, el A, por ejemplo, no fuera divisible por r, daríamos á x un valor no divisible por r, y á y, por el contrario, otro valor divisible por r; y, si los dos coeficientes A y C fuesen divisibles por r, el B no podria serlo, y bastaba entónces para lograr nuestro objeto atribuir á las dos variables x é y valores no divisibles tampoco por r.

De aquí se desprende primeramente, que *los valores para x é y pueden escogerse de modo que el resultante para F sea primo con un número cualquiera determinado k:* puesto que entónces la cuestion estriba en lograr que F no sea divisible por ninguno de los factores primos r', r'', r'''..... de k; y esto se consigue, segun lo dicho antes, haciendo que las dos variables x é y sean divisibles por alguno de aquellos factores, y no lo sean por los restantes: condiciones que siempre pueden de infinitos modos realizarse.

En segundo lugar, *las variables x é y pueden escogerse de modo que el valor para F resulte positivo.* En cuanto á las formas con determinante negativa no hay duda ninguna; porque sólo tratamos de las formas de este género, cuyos coeficientes extremos fuesen positivos; y, respecto de las formas con determinante positiva, como se verifica para ellas la ecuacion

$$a\sigma F = (ax + by)^2 - Dy^2,$$

sólo deberemos procurar elegir entre los valores para x é y, que cumplan ya con la condicion precedente, aquellos que produzcan para la expresion $(ax + by)$ un valor absoluto, mayor ó menor que $y\sqrt{D}$, segun que a sea positivo ó negativo.

Últimamente: todavía se les puede imponer *á los valores de x é y la condicion de ser primos entre sí*, sin perjuicio de que cumplan con las precedentes: de convertir el valor de F en positivo, y primo con cualquier número k; pues en el caso de que los valores para x é y, elegidos con sujecion á estas últimas, tuviesen algun divisor comun, no habria inconveniente en dividirlos por él, y los cocientes resultantes, ya primos entre sí, satisfarian evidentemente á todas las condiciones enumeradas.

Hagamos ahora una aplicacion de esta doctrina general á un caso particular, que nos será útil en lo sucesivo, para dejar, por otra parte, del todo resuelta, la cuestion en un principio enunciada. En el caso especial de ser $k = 2D$, y (a, b, c) una forma cualquiera de divisor σ, y determinante D, podrán siempre encontrarse dos números, primos entre sí, α y γ, que, sustituidos en la expresion

$$\frac{a\alpha^2 + 2b\alpha\gamma + c\gamma^2}{\sigma} - \frac{a'}{\sigma},$$

produzcan para ella un valor *positivo y primo con* $2D$. Ahora bien, probada la existencia de los dos números α y γ, mediante la ecuacion $\alpha\delta - \beta\gamma = 1$ podremos determinar (69) otros dos cualesquiera β y δ; y entónces la forma (a, b, c), por la sustitucion $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$, se con-

vertirá en otra equivalente, cuyo primer coeficiente a', será positivo, y además el cociente $a' : \sigma$ primo con $2D$: con lo cual queda demostrado que las formas representantes de cada una de las clases en que se distribuye un sistema S pueden siempre elegirse sujetas á esta nueva condicion.

168.—*Distribucion de los números constructores en un número determinado de séries aritméticas pareadas.*

En conformidad con lo que acabamos de decir, admitamos desde luego que la forma (a, b, c), representante de su clase, está elegida con la condicion de que el cociente $a : \sigma$ sea, no solo positivo, sino además primo con $2D$. ¿Cuál será ahora el sistema de los pares de valores (x, y) que convierten la expresion *(Condicion I)*

$$\frac{a x^2 + 2 b x y + c y^2}{\sigma}$$

en otro sistema correspondiente de valores primos con $2D$?

Designando, como siempre, por Δ el valor absoluto de la determinante D, podremos establecer las fórmulas para x é y,

$$x = 2\Delta v + \alpha \qquad y = 2\Delta w + \gamma,$$

en las que α y γ representan cualquiera de los 2Δ números,

$$0,\ 1,\ 2,\ \ldots\ldots\ (2\Delta - 1),$$

y v y w, dos enteros cualesquiera; y por cuyo medio sólo de un modo puede ser expresada cada combinacion de los valores para x é y. De las congruencias consiguientes,

$$x \equiv \alpha \pmod{2\Delta}. \qquad y \equiv \gamma \pmod{2\Delta}.$$

se deduce esta otra:

$$\frac{a x^2 + 2 b x y + c y^2}{\sigma} \equiv \frac{a \alpha^2 + 2 b \alpha \gamma + c \gamma^2}{\sigma} \pmod{2 \Delta}$$

la cual manifiesta que entre todas las $(2\Delta)^2 = 4\Delta^2$ combinaciones (α, γ), solamente admitamos aquellas que hagan primo con $2D$ el valor de la expresion

$$\frac{a \alpha^2 + 2 b \alpha \gamma + c \gamma^2}{\sigma}.$$

Las combinaciones (x, y), así encontradas, se distribuyen entónces en un número de pares de séries aritméticas, cuya diferencia es 2Δ, y cuyos primeros términos α, γ constituyen á su vez combinaciones especiales del mismo género, sujetas á la misma condicion. Lo que más nos interesa ahora no es hallar estas combinaciones (α, γ), sino su número solamente; porque este número es el que nos ha de servir en adelante para determinar el que principalmente buscamos. Para hallarlo examinaremos diferentes casos.

1.° $\sigma = 1$. La cuestion que en este tratamos de resolver puede formularse en los siguientes términos: ¿cuál es el número de combinaciones (α, γ) que convierten la expresion $a\alpha^2 + 2b\alpha\gamma + c\gamma^2$, ó bien, como a es primo con 2Δ, esta otra

$$a(a\alpha^2 + 2b\alpha\gamma + c\gamma^2) = (a\alpha + b\gamma)^2 \pm \Delta\gamma^2,$$

en números primos con 2Δ? Para contestar á esta pregunta sustituyamos primeramente por γ cualquiera de los Δ números pares

$$0, 2, 4, 6, \ldots\ldots (2\Delta - 2).$$

En tal supuesto, si la expresion

$$(a\alpha + b\gamma)^2 \pm \Delta\gamma^2$$

ha de tomar un valor primo con 2Δ, es necesario y suficiente que $(a\alpha + b\gamma)^2$, ó $(a\alpha + b\gamma)$ sea primo con 2Δ. Mas, si conservando γ un valor determinado de los escritos antes, recibe α sucesivamente los del sistema completo de restos (mod. 2Δ)

$$0,\ 1,\ 2,\ 3,\ \ldots\ldots\ (2\Delta - 1),$$

la expresion $(a\alpha + b\gamma)$ producirá tambien, por ser a primo con el módulo 2Δ, un sistema completo de restos, segun el mismo módulo (63); y, por consecuencia, á cada valor par de los atribuidos á γ corresponderán $\varphi(2\Delta)$ posibles para α, significando φ lo que casi siempre (55). Demos ahora á γ cualquiera de los Δ valores impares

$$1,\ 3,\ 5,\ 7,\ \ldots\ldots\ (2\Delta - 1).$$

Entónces, si Δ es par, la condicion para que

$$(a\alpha + b\gamma)^2 \pm \Delta\gamma^2$$

sea primo con 2Δ, se reduce á que $(a\alpha + b\gamma)$ lo sea; y, por lo tanto, α puede recibir $\varphi(2\Delta)$ valores como antes. Si Δ, por el contrario, y $\Delta\gamma^2$, en consecuencia, fuesen impares, la expresion

$$(a\alpha + b\gamma)^2 \pm \Delta\gamma^2$$

deberá ser entónces impar y primo con Δ, y para esto $(a\alpha + b\gamma)$ par y primo con Δ, y, lo mismo de consiguiente, el resto (mod. 2Δ) de $(a\alpha + b\gamma)$; y recíprocamente: siendo par y primo con Δ el resto (mod. 2Δ) de $(a\alpha + b\gamma)$, la condicion principal, antes enunciada, quedará cumplida. Ahora bien, si atribuimos á α todos sus 2Δ valores, los restos de $(a\alpha + b\gamma)$ recorrerán estos mismos 2Δ valores, entre los cuales existirán los Δ siguientes, pares,

$$0,\ 2,\ 4,\ \ldots\ldots\ 2(\Delta - 1),$$

y entre estos últimos $\varphi(\Delta)$ primos con el número impar Δ. Este nú-

mero, $\varphi(\Delta)$, es, por consecuencia, tambien el de los valores posibles de α, correspondientes á cada uno de los impares, atribuidos á γ; y, por ser Δ impar y primo con 2, es lo mismo que $\varphi(2\Delta)$. Luego, en todos los casos, á cada valor, par ó impar, de γ, corresponden $\varphi(2\Delta)$ de α, que convierten la expresion

$$(a\alpha + b\gamma)^2 \pm \Delta\gamma^2$$

en números primos con 2Δ; y, siendo 2Δ el conjunto de los valores de γ, el completo de las combinaciones (α, γ) será finalmente:

$$2\Delta\varphi(2\Delta).$$

2.° Sea $\sigma = 2$, a y c pares, b impar, y $D \equiv 1 \pmod 4$. ¿Cuántas serán, en este caso, las combinaciones (α, γ) que conviertan la expresion

$$\frac{a\alpha^2 + 2b\alpha\gamma + c\gamma^2}{2} = \frac{1}{2}a\alpha^2 + b\alpha\gamma + \frac{1}{2}c\gamma^2$$

en números primos con Δ? Concretémonos primeramente á las combinaciones (α, γ) que produzcan para la expresion última valores impares. Como somos dueños de elegir la forma, representante de su clase, (a, b, c), de modo que $\frac{1}{2}a$ sea primo con 2Δ, é impar en consecuencia, la determinante referida á tal forma, $D = b^2 - ac$, será

$$\equiv 1, \quad \text{ó} \quad \equiv 5 \pmod 8,$$

segun que $\frac{1}{2}c$ sea par, ó impar. En el primer supuesto, si la expresion

$$\frac{1}{2}a\alpha^2 + b\alpha\gamma + \frac{1}{2}c\gamma^2$$

ha de resultar impar, debe ser $\frac{1}{2}a\alpha^2 + b\alpha\gamma = a(\frac{1}{2}a\alpha + b\gamma)$ impar;

y para esto es indispensable que sea precisamente α impar, y par γ; en el segundo, uno cualquiera de los dos números α ó γ, por lo ménos, debe ser impar. Y, como á cada uno de los Δ valores impares precisamente que puede recibir α corresponden Δ pares de γ, será $\Delta \times \Delta = \Delta^2$ el número de las combinaciones posibles (α, γ), en el primer caso; y agregando á este número el $2\Delta^2$, que resulta de suponer á γ, por ejemplo, impar, y que α recorra todos sus 2Δ valores, se obtendrá el $3\Delta^2$, para el número de combinaciones posibles (α, γ), en el segundo.

Exijamos ahora que las combinaciones (α, γ), no sólo produzcan para la expresion $\frac{1}{2} a\alpha^2 + b\alpha\gamma + \frac{1}{2} c\gamma^2$ valores impares, sino además primos con Δ. Para satisfacer á esta exijencia es necesario y suficiente que el valor de

$$(a\alpha + b\gamma)^2 \pm \Delta\gamma^2 = 2a\left(\tfrac{1}{2} a\alpha^2 + b\alpha\gamma + \tfrac{1}{2} c\gamma^2\right)$$

ó, de consiguiente, el de $(a\alpha + b\gamma)$ sea primo con Δ. Esto pide en el primer caso, cuando $D \equiv 1 \pmod 8$, que γ reciba valores pares exclusivamente, y α impares. Si, pues, damos á γ uno determinado de los Δ siguientes

$$0,\ 2,\ 4,\ \ldots\ldots\ (2\Delta - 2),$$

mientras α recorra todos los Δ impares

$$1,\ 3,\ 5,\ \ldots\ldots\ (2\Delta - 1),$$

que constituyen evidentemente un sistema completo de restos (mod. Δ), la expresion $(a\alpha + b\gamma)$, como α es primo con Δ, tomará Δ valores que á su vez forman un sistema completo de restos, segun el mismo módulo Δ, entre los cuales existirán $\varphi(\Delta) = \varphi(2\Delta)$ primos con Δ. Y, por consecuencia, existen entónces $\Delta\varphi(2\Delta)$ combinaciones posibles (α, γ). En el segundo caso, cuando $D \equiv 5 \pmod 8$, y uno, por lo ménos, de los dos números α, γ debe ser impar, se halla primeramente, como antes, que á cada valor, par, de γ corresponden $\varphi(\Delta) = \varphi(2\Delta)$

impares de α; y, por consecuencia, que el número total de combinaciones posibles (α, γ) es tambien $\Delta\varphi(2\Delta)$. Pero, si γ fuese impar, y α recorriera sus 2Δ valores, como puede tambien ocurrir sin faltar á la condicion impuesta, la expresion $(a\alpha + b\gamma)$ tomaria dos veces el mismo sistema completo de restos (mod. Δ); á cada uno de los Δ impares valores de γ corresponderian, por lo tanto, $2\varphi(\Delta) = 2\varphi(2\Delta)$ posibles de α; y el número total de combinaciones (α, γ) seria entónces $2\Delta\varphi(2\Delta)$. Y sumado este número con el anterior, resultan $3\Delta\varphi(2\Delta)$ combinaciones posibles en el caso que estamos estudiando.

Resumiendo: el número total de pares de séries aritméticas, entre sí correspondientes,

$$x = 2\Delta v + \alpha, \qquad y = 2\Delta w + \gamma,$$

que satisfacen á la condicion I, tantas veces recordada, tiene por expresion

$$\omega \cdot \Delta\varphi(2\Delta),$$

en la cual:

$\omega = 2$, cuando sea $\sigma = 1$

$\omega = 1$, cuando $\sigma = 2$, y $D \equiv 1 \pmod 8$

$\omega = 3$, cuando $\sigma = 2$, y $D \equiv 5 \pmod 8$.

LÍMITES DE LOS DOS MIEMBROS DE LA ECUACION FUNDAMENTAL.

Volvamos nuevamente sobre la ecuacion fundamental. Haciendo en ella $s = 1 + \rho$, multiplicándola por ρ, y dividiéndola por $\sigma^{1+\rho}$, toma la forma:

$$\rho\Sigma\frac{1}{(ax^2 + 2bxy + cy^2)^{1+\rho}} + \ldots\ldots = \frac{\rho\varkappa}{\sigma^{1+\rho}}\Sigma\frac{1}{n^{1+\rho}}\Sigma\left(\frac{D}{n}\right)\frac{1}{n^{1+\rho}}.$$

Y en esta forma, suponiendo que el número positivo ρ es infinitamente pequeño, vamos á determinar los límites de cada uno de los términos que en sus dos miembros figuran.

169.—*Límite del primer miembro para las determinantes negativas.*

Sea, como siempre, $D = -\Delta$. Las variables x é y comprendidas en la suma principal, relativa á la forma (a, b, c), sólo tienen entónces que satisfacer á la condicion I; y acabamos de probar que tal suma puede descomponerse en $\omega \Delta \varphi(2\Delta)$ séries parciales, correspondientes á cada una de las combinaciones posibles (α, γ). Consideremos, pues, primeramente una sola suma principal,

$$\rho \sum \frac{1}{(a x^2 + 2 b x y + c y^2)^{1+\rho}},$$

en la que puedan recibir las variables x é y todos los valores

$$x = 2\Delta v + \alpha, \qquad y = 2\Delta w + \gamma$$

correspondientes á una combinacion posible, determinada, (α, γ), y á todos los valores enteros imaginables de v y de w. El límite del producto que constituye la suma principal expresada es idéntica (*) al del cociente $T : t$, cuyo divisor t representa un número positivo, superior á todo límite, ó infinitamente grande; y cuyo dividendo T designa el conjunto de los números construidos por la forma (a, b, c), que no serán mayores que t, y deberán, por lo tanto, satisfacer á la condicion

$$a x^2 + 2 b x y + c y^2 \leq t,$$

ó bien, en otra forma, á la

(*) Apéndice II.

$$a\left(\frac{x}{\sqrt{t}}\right)^2 + 2b\frac{x}{\sqrt{t}}\cdot\frac{y}{\sqrt{t}} + c\left(\frac{y}{\sqrt{t}}\right)^2 \leqq 1.$$

El límite del cociente $T:t$ se determina con facilidad mediante una consideracion geométrica. Hagamos, en efecto,

$$\frac{x}{\sqrt{t}} = \xi, \qquad \frac{y}{\sqrt{t}} = \eta;$$

el dividendo T expresará entónces el número de pares de valores

$$\xi = \frac{2\Delta}{\sqrt{t}}v + \frac{\alpha}{\sqrt{t}}, \qquad \eta = \frac{2\Delta}{\sqrt{t}}w + \frac{\beta}{\sqrt{t}} \tag{1}$$

sujetos á la condicion

$$a\xi^2 + 2b\xi\eta + c\eta^2 \leqq 1. \tag{2}$$

Mirando ahora á ξ, η como las coordenadas rectangulares de un punto en un plano, y dando á v y w los valores de la série entera, los puntos (ξ, η), determinados sucesivamente por las fórmulas (1), formarán una cuadrícula, constituida evidentemente por los dos sistemas de rectas paralelas á cada uno de los dos ejes de coordenadas; siendo $\delta = 2\Delta:\sqrt{t}$ la distancia constante entre cada dos paralelas inmediatas del uno y el otro sistema. De este modo queda dividido el plano en cuadraditos, cuya área comun es

$$\delta^2 = \frac{4\Delta^2}{t},$$

y cuyos vértices son precisamente los puntos (ξ, η); y T, por consecuencia, representará el número de puntos de la mencionada cuadrícula que no caigan fuera de la curva expresada por la ecuacion

$$a\xi^2 + 2b\xi\eta + c\eta^2 = 1. \qquad (3)$$

Mas esta ecuacion de segundo grado, por ser $b^2 - ac = -\Delta$ (negativo), y a positivo, es la de una elipse cuyo centro coincide con el orígen de coordenadas. El producto

$$T \cdot \delta^2 = 4\Delta^2 \cdot \frac{T}{t}$$

tiene por límite el área A, de tal elipse, en el supuesto de ser t infinitamente grande, y δ, por lo tanto, infinitamente pequeño (Ap. III); y el límite de que se trata será, por consecuencia:

$$\text{lím.} \frac{T}{t} = \frac{A}{4\Delta^2}.$$

Este límite, segun su expresion manifiesta, es independiente de la combinacion (α, γ), y el mismo, de consiguiente, para todas las $\omega\Delta\varphi(2\Delta)$ sumas parciales que componen la principal considerada: de lo cual resulta que esta suma principal, perteneciente á la forma (a, b, c), tendrá por límite

$$\omega\Delta\varphi(2\Delta) \cdot \frac{A}{4\Delta^2} = \frac{\omega\varphi(2\Delta)}{4\Delta} A;$$

donde A designa el área de la elipse (3), que nos resta determinar.

Con este objeto trasformemos la ecuacion (3), refiriéndola á los ejes principales de la elipse que representa, como nuevos ejes de coordenadas; la nueva ecuacion de la elipse, referida á sus ejes será:

$$a'\xi'^2 + c'\eta'^2 = 1;$$

y, como en esta trasformacion de coordenadas rectangulares, la determinante $b^2 - ac$, permanece invariable, y, por consecuencia,

$$a' c' - a c - b^2 = \Delta;$$

y, por otra parte, $\sqrt{a'}$ y $\sqrt{c'}$ son los valores recíprocos de los semiejes de dicha elipse, el área que buscamos será:

$$A = \frac{\pi}{\sqrt{a' c'}} = \frac{\pi}{\sqrt{\Delta}}.$$

tomando siempre, por supuesto, la raiz cuadrada *positiva*. Con este valor de A se halla finalmente que el valor del límite de la suma principal

$$\rho \Sigma \frac{1}{(a x^2 + 2 b x y + c y^2)^{1+\rho}},$$

perteneciente á la forma (a, b, c), tiene por expresion

$$\frac{\omega \pi \varphi (2 \Delta)}{4 \Delta \sqrt{\Delta}};$$

la cual, y esto merece notarse, es independiente de los coeficientes a, b, c, y, por lo tanto, de la individual naturaleza de dicha forma.

Ahora bien, al mismo límite se aproximará cualquiera otra suma principal, perteneciente á otra forma (a', b', c'), de las que constituyen el sistema *S:* luego, designando por h el número de las sumas principales que figuran en el primer miembro de la ecuacion fundamental, ó, lo que es igual, *el número de clases de formas no equivalentes, de especie* σ, *para la determinante* $D = -\Delta$, el límite de todo el primer miembro mencionado será en conclusion:

$$\frac{\omega \pi \varphi (2 \Delta)}{4 \Delta \sqrt{\Delta}} h.$$

170. — *Límite del segundo miembro para las determinantes negativas. — Número de clases de formas.*

Vamos á estudiar ahora el segundo miembro de la ecuacion fundamental, y á buscar el límite del producto en él comprendido,

$$\rho \Sigma \frac{1}{n^{1+\rho}},$$

donde el signo sumatorio se refiere á todos los valores enteros, positivos y primos con 2Δ. Designando por $\nu, \nu', \nu'', \ldots\ldots$ los $\varphi(2\Delta)$ primeros de estos números, esto es, los menores que 2Δ, la suma propuesta podremos descomponerla en $\varphi(2\Delta)$ sumas parciales de la forma

$$\rho \left\{ \frac{1}{\nu^{1+\rho}} + \frac{1}{(\nu+2\Delta)^{1+\rho}} + \frac{1}{(\nu+4\Delta)^{1+\rho}} + \frac{1}{(\nu+6\Delta)^{1+\rho}} + \ldots\ldots \right\}$$

en la que los términos afectados por el exponente $(1+\rho)$ constituyen en cada caso una série aritmética, cuya diferencia es 2Δ. Ahora bien, el límite de cada una de estas sumas parciales es (Apénd. II)

$$= \frac{1}{2\Delta};$$

y, como es independiente de ν, el de las $\varphi(2\Delta)$ sumas parciales, ó el de la suma entera, será evidentemente

$$= \frac{\varphi(2\Delta)}{2\Delta};$$

y este mismo el del segundo miembro de la ecuacion fundamental

$$= \frac{\varkappa \varphi(2\Delta)}{\sigma 2\Delta} \lim. \Sigma \left(\frac{D}{n}\right) \frac{1}{n^{1+\rho}}.$$

Pero los dos miembros de la mencionada ecuacion fundamental, para valores de s superiores á la unidad, ó lo que es igual, para valores positivos de ρ, son idénticos; y lo mismo pasará con sus límites respectivos: luego no hay inconveniente en establecer la igualdad

$$\frac{\omega \pi \varphi(2\Delta)}{4\Delta\sqrt{\Delta}} h = \frac{\varkappa \varphi(2\Delta)}{\sigma . 2\Delta} \lim. \Sigma \left(\frac{D}{n}\right) \frac{1}{n^{1+\rho}}$$

de la cual, despejando h, despues de restablecer el valor $D = -\Delta$, resulta:

$$h = \frac{2\varkappa}{\sigma \omega \pi} \sqrt{-D} . \lim. \Sigma \left(\frac{D}{n}\right) \frac{1}{n^{1+\rho}}$$

para la expresion del número de clases de formas primitivas de especie σ (con coeficientes extremos positivos) para la determinante *negativa*, $D = -\Delta$.

En esta expresion sabemos además que, por una parte (162):

$$\varkappa = 4, \text{ cuando } D = -1$$

$$\varkappa = 6, \text{ cuando } D = -3 \text{ y } \sigma = 2$$

$$\varkappa = 2, \text{ en todos los demás casos;}$$

y por otra (168):

$$\omega = 2, \text{ cuando } \sigma = 1$$

$$\omega = 1, \text{ cuando } \sigma = 2 \text{ y } D \equiv 1 \pmod 8$$

$$\omega = 3, \text{ cuando } \sigma = 2 \text{ y } D \equiv 5 \pmod 8.$$

171.—*Relacion entre los números de clases de formas de la primera, y de la segunda especie, para una determinante negativa.*

En la fórmula general para h sustituyamos los valores particulares $\sigma = 1$, $\varkappa = 2$, $\omega = 2$, que corresponden á las formas de la primera especie; el número de clases para estas formas será, por consecuencia:

$$h = \frac{2}{\pi}\sqrt{-D}\,.\,\text{lím.}\,\Sigma\left(\frac{D}{n}\right)\frac{1}{n^{1\cdot\rho}}\,.$$

con la única excepcion de $D = -1$ para cuya determinante es $\varkappa = 4$.

La fórmula general para la determinante $D = -1$ se convierte en esta otra:

$$h = \frac{4}{\pi}\,\text{lím.}\,\Sigma\left(\frac{D}{n}\right)\frac{1}{n^{1\cdot\rho}}\,.$$

ó bien, poniendo por el símbolo de Legendre su valor explícito (119-1.°)

$$h = \frac{4}{\pi}\,\text{lím.}\,\Sigma\,\frac{(-1)^{\frac{1}{2}(n-1)}}{n^{1\cdot\rho}}\,.$$

Pero más adelante demostraremos, en general, que:

$$\text{lím.}\,\Sigma\left(\frac{D}{n}\right)\frac{1}{n^{1+\rho}} = \Sigma\left(\frac{D}{n}\right)\frac{1}{n}:$$

luego, efectuando la sumacion así resultante $\Sigma\,(-1)^{\frac{1}{2}(n-1)}:n$, para lo cual basta sustituir n por la série de los números impares, primos con 2, se obtiene por fin:

$$h = \frac{4}{\pi}\left(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots\ldots\right) = 1,$$

en atencion á que la série inclusa en el paréntesis, llamada de *Leibnitz*, tiene por valor $\frac{1}{4}\pi$. Y este resultado viene á confirmar de nuevo el principio antes establecido (148) de que, para la determinante $D = -1$, sólo existe una clase de formas (con los coeficientes extremos positivos).

Para deducir de la fórmula general de h el valor particular h' de este número, respecto de las formas de segunda especie, debemos distinguir los dos casos, $D \equiv 1 \pmod 8$, y $D \equiv 5 \pmod 8$, para los que ω toma, como sabemos, valores diferentes. En el primero, es $\varkappa = 2$, $\omega = 1$; y, por consiguiente:

$$h' = \frac{2}{\pi}\sqrt{-D} \cdot \lim. \sum \left(\frac{D}{n}\right)\frac{1}{n^{1-\rho}}$$

ó igual al número que encontramos relativo á las de primera especie. En el segundo, $\varkappa = 2$, $\omega = 3$, y, por tanto:

$$h' = \frac{1}{3} \cdot \frac{2}{\pi}\sqrt{-D} \cdot \lim. \sum \left(\frac{D}{n}\right)\frac{1}{n^{1-\rho}}$$

ó igual al tercio del correspondiente á las de primera especie; con la única excepcion $D = -3$, en que $\varkappa = 6$; pues, para este valor particular de la determinante, se confunden de nuevo los números de clases de formas, sean éstas de la primera, ó de la segunda especie.

En resúmen: designando por h el número de tales clases para las formas de primera especie, y por h' el referente á las de segunda, tenemos:

$h' = h$, cuando $D \equiv 1 \pmod 8$, y para $D = -3$.

$h = \frac{1}{3}h$, cuando $D \equiv 5 \pmod 8$, exceptuando $D = -3$.

172.—*Límite del primer miembro de la ecuacion fundamental para las determinantes positivas.—Número de clases de formas.*

Sea, pues, $D = \Delta$. Conforme hicimos al tratar de las determinantes negativas, descompongamos cada suma principal, de las que constituyen el primer miembro en cuestion, correspondiente á una forma determinada (a, b, c), en $\omega \Delta^{\rho}(2\Delta)$ sumas parciales, de la forma

$$\rho \Sigma \frac{1}{(a x^2 + 2 b x y + c y^2)^{1+\rho}},$$

en la cual pueden recibir las variables x é y todos los pares de valores,

$$x = 2\Delta v + \alpha, \qquad y = 2\Delta w + \gamma, \tag{1}$$

pertenecientes á una combinacion determinada (α, γ) y á todos los enteros imaginables v y w. Pero dichas variables, respecto de las determinantes positivas, deben satisfacer además á las condiciones aisladoras II (162),

$$y \geqq 0, \qquad a x + b y > \frac{T}{U} y \tag{2}$$

de cuya restriccion, á primera vista inconveniente, se deduce, por el contrario, que (134) los dos factores

$$a x + (b + \sqrt{D})\, y, \qquad a x + (b - \sqrt{D})\, y,$$

y, de resultas, la forma:

$$a x^2 + 2 b x y + c y^2$$

deben ser números positivos: circunstancia que nos permite aplicar

ahora tambien los principios expuestos (Ap. II), y aplicados antes, al estudiar las formas con determinantes negativas. Por consecuencia, si designamos por t un número cualquiera positivo, y por τ el número de los pares de valores (x, y), compendiados en las séries (1), y que satisfacen á las condiciones (2), y además á esta otra

$$a x^2 + 2 b x y + c y^2 \leqq t, \tag{3}$$

sólo tendremos que buscar aquí el límite del cociente $\tau : t$, en el supuesto de que t crezca indefinidamente; pues este límite es al mismo tiempo el de la suma parcial anterior, correspondiente á una combinacion (α, γ). Para hallar dicho límite establezcamos, como anteriormente, las ecuaciones

$$\xi = \frac{x}{\sqrt{t}}, \qquad \eta = \frac{y}{\sqrt{t}},$$

en las cuales $\sqrt{t}$ significa la raiz positiva. Mirando á (ξ, η) como las coordenadas de un punto en un plano, τ representará el número de los puntos de cuadrícula, contenidos en las dos séries

$$\xi = \frac{2\Delta}{\sqrt{t}} v + \frac{\alpha}{\sqrt{t}}, \qquad \eta = \frac{2\Delta}{\sqrt{t}} w + \frac{\gamma}{\sqrt{t}},$$

que satisfacen á las condiciones

$$\eta \geq 0, \qquad a\xi + b\eta > \frac{T}{\sqrt{t}} \eta,$$

$$a\xi^2 + 2b\xi\eta + c\eta^2 \leqq 1:$$

esto es, el número de aquellos puntos encerrados, sobre el plano de las $\xi\eta$, de un lado, por el eje ξ; de otro, por una recta que pasa por el orígen de coordenadas; y finalmente, por una rama de hipérbola, cuyo centro coincide con dicho orígen. Designando por B el área de la porcion del plano de las $\xi\eta$ así limitada, y aplicando los principios ci-

tados (Ap. III), en la suposicion de ser t infinitamente grande, y el lado $\delta = 2\Delta : \sqrt{t}$, de los cuadraditos de la cuadrícula, por lo tanto, infinitamente pequeño, tendremos:

$$\text{lím. } \tau \,.\, \delta^2 = 4\Delta^2 \,.\, \text{lím. } \frac{\tau}{t} = B,$$

de donde:

$$\text{lím. } \frac{\tau}{t} = \frac{B}{4\Delta^2}.$$

Y, como este límite es juntamente, segun dijimos, el de la suma parcial propuesta, correspondiente á una combinacion, (α, γ), y en él no figuran para nada estos valores α, y γ, resulta que será el mismo tambien para todas las $\omega\Delta\varphi(2\Delta)$ sumas parciales, pertenecientes á las diversas combinaciones (α, γ), que componen la suma principal, relativa á la forma (a, b, c); y, por consecuencia:

$$\frac{\omega\varphi(2\Delta)}{4\Delta} B$$

expresará efectivamente el límite de aquella suma total

$$\rho \Sigma \frac{1}{\left(a x^2 + 2 b x y + c y^2\right)^{1 \cdot \rho}}.$$

Nos falta determinar todavía el área B, del sector hiperbólico, definido por las tres desigualdades ó condiciones anteriormente escritas. Estas condiciones de limitacion, mediante las fórmulas conocidas de trasformacion de coordenadas rectilíneas en polares,

$$\xi = r \cos.\ \varphi, \qquad \eta = r \text{ sen. } \varphi,$$

se convierten en las siguientes:

$$\text{sen.}\,\varphi \gtrless 0, \qquad a\,\text{cotang.}\,\varphi + b > \frac{T}{U}$$

$$r^2\,(a\,\text{cos.}^2\varphi + 2\,b\,\text{cos.}\,\varphi\,\text{sen.}\,\varphi + c\,\text{sen.}^2\varphi) \leqq 1.$$

Y de las dos primeras se deduce, como advertimos antes, que las cantidades

$$a\,\text{cos.}\,\varphi + (b + \sqrt{D})\,\text{sen.}\,\varphi, \qquad a\,\text{cos.}\,\varphi + (b - \sqrt{D})\,\text{sen.}\,\varphi,$$

$$a\,\text{cos.}^2\varphi + 2\,b\,\text{cos.}\,\varphi\,\text{sen.}\,\varphi + c\,\text{sen.}^2\varphi,$$

deben ser positivas para todo ángulo φ que las satisfaga: lo cual significa que dentro del espacio angular, por dichas dos condiciones definido, no puede caer ninguna asíntota, sino, por el contrario, un trozo limitado de hipérbola, y, como consecuencia, que el sector de que se trata es asimismo finito. Aclarado este punto, el área que buscamos se halla por la expresion conocida

$$B = \int\int r\,d\,r\,d\,\varphi = \tfrac{1}{2}\int r^2\,d\,\varphi.$$

Esta integral pide, en primer término, que pongamos en ella por r^2 su valor en funcion de la otra variable φ. Tomando, pues, el valor del radio r que corresponde á la misma rama de la hipérbola, tendremos:

$$r^2 = \frac{1}{a\,\text{cos.}^2\varphi + 2\,b\,\text{cos.}\,\varphi\,\text{sen.}\,\varphi + c\,\text{sen.}^2\varphi},$$

ó, descomponiendo el denominador, y separando luego factores comunes:

$$r^2 = \frac{a}{2\sqrt{D}}\left\{\frac{1}{a\,\text{cotang.}\,\varphi + b - \sqrt{D}} - \frac{1}{a\,\text{cotang.}\,\varphi + b + \sqrt{D}}\right\}\frac{1}{\text{sen.}^2\varphi}.$$

Antes de sustituir en la integral ya sencilla, antes escrita, conviene advertir que

$$\frac{d\varphi}{\text{sen.}^2\varphi} = -d\,.\,\text{cotang.}\,\varphi:$$

de modo que, si consideramos á cotang. φ como nueva variable, la integral pedida será:

$$\frac{1}{2}\int r^2 d\varphi = \frac{1}{4\sqrt{D}}\int \frac{a\,d\,.\,\text{cotang.}\,\varphi}{a\,\text{cotang.}\,\varphi + b + \sqrt{D}} - \frac{1}{4\sqrt{D}}\int \frac{a\,d\,.\,\text{cotang.}\,\varphi}{a\,\text{cotang.}\,\varphi + b - \sqrt{D}}$$

$$= \frac{1}{4\sqrt{D}}\,\text{log.}\,\frac{a\,\text{cotang.}\,\varphi + b + \sqrt{D}}{a\,\text{cotang.}\,\varphi + b - \sqrt{D}}.$$

Ahora bien, esta integral debe comprender todos los valores de φ cuyos senos sean positivos, y extenderse, en consecuencia, desde $\varphi = 0$ hasta el valor de φ que verifique la igualdad $U(a\,\text{cotang.}\,\varphi + b) = T$: límite este último completamente determinado por la condicion de ser sen. φ positivo; y, como ya antes indicamos que, dentro de todo este espacio angular, las cantidades

$$a\,\text{cotang.}\,\varphi + b + \sqrt{D} \qquad \text{y} \qquad a\,\text{cotang.}\,\varphi + b - \sqrt{D}$$

conservan siempre su signo positivo, resulta que la integral indefinida anterior representa una funcion real y contínua de φ, que solamente podemos definir, en consecuencia, por los dos límites mencionados. Efectuándolo así, esto es, verificando la integracion entre los límites $\varphi = 0$, y $\varphi =$ al valor que satisface á la condicion $U(a\,\text{cotang.}\,\varphi + b) = T$; y, teniendo presente que $T^2 - DU^2 = (T + U\sqrt{D})(T - U\sqrt{D}) = \sigma^2$, se obtiene por último:

$$B = \frac{1}{4\sqrt{D}}\,\text{log.}\,\frac{T + U\sqrt{D}}{T - U\sqrt{D}} = \frac{1}{2\sqrt{D}}\,\text{log.}\,\frac{T + U\sqrt{D}}{\sigma}.$$

Con este valor de B, el límite de la suma principal, correspondiente á la forma (a, b, c), despues de escribir D por Δ, se expresa como sigue:

$$\frac{\omega\,\varphi\,(2\,D)}{8\,D\sqrt{D}}\log.\frac{T+U\sqrt{D}}{\sigma}.$$

donde T, U, representan, como siempre, los dos mínimos enteros, positivos, que satisfacen á la ecuacion $T^2 - D\,U^2 = \sigma^2$.

Esta expresion manifiesta, como la relativa á las determinantes negativas, que el límite de una suma principal, perteneciente á cualquiera forma (a, b, c) del sistema S, depende exclusivamente de la determinante D y de la especie σ; y no, por lo tanto, de la particular naturaleza de cada forma: lo cual quiere decir que es el mismo para todas ellas. Significando, pues, por h el conjunto de todas las formas comprendidas en el sistema S, ó *el número de todas las clases de formas primitivas, de especie* σ, *para la determinante positiva* D,

$$h\,\frac{\omega\,\varphi\,(2\,D)}{8\,D\sqrt{D}}\log.\frac{T+U\sqrt{D}}{\sigma}$$

será el límite á que se aproxima el primer miembro de la ecuacion fundamental, á condicion de que el valor positivo de φ decrezca indefinidamente.

Respecto del segundo miembro sólo debemos observar que, para las determinantes positivas, es $\varkappa = 1$ (162); y por consecuencia, será tambien ahora, como para las formas con determinante negativa:

$$\text{lím.}\,\rho\,\Sigma\,\frac{1}{n^{1+\rho}} = \frac{\varphi\,(2\,\Delta)}{2\,\Delta} = \frac{\varphi\,(2\,D)}{2\,D},$$

y el límite de todo el segundo miembro de la ecuacion fundamental:

$$\frac{\varphi\,(2\,D)}{\sigma\,.\,2\,D}\,\text{lím.}\,\Sigma\left(\frac{D}{n}\right)\frac{1}{n^{1+\rho}}.$$

Igualando este límite al del primer miembro, arriba escrito, y despejando h de la igualdad resultante, se obtiene para el número h la expresion:

$$h = \frac{1}{\sigma\omega} \cdot \frac{4\sqrt{D}}{\log. \frac{T + U\sqrt{D}}{\sigma}} \cdot \text{lím.} \Sigma \left(\frac{D}{n}\right) \frac{1}{n^{1+\rho}}.$$

173.—*Relacion entre los números de clases de formas de la primera, y la segunda especie, para una determinante positiva.*

Para obtener la expresion del número h, correspondiente á las formas primitivas, de la primera especie, deberemos hacer $\sigma = 1$ y $\omega = 2$ en la general precedente, y así hallamos:

$$h = \frac{2\sqrt{D}}{\log. (T + U\sqrt{D})} \cdot \text{lím.} \Sigma \left(\frac{D}{n}\right) \frac{1}{n^{1+\rho}};$$

donde T, U representan, como sabemos, la solucion mínima de la ecuacion

$$T^2 - D\,U^2 = 1.$$

Para que existan formas de segunda especie, respecto de la determinante D, es necesario ante todo (140) que sea $D \equiv 1 \pmod 4$.

Admitida esta condicion, y haciendo $\sigma = 2$ en la expresion general de h, se halla desde luego:

$$h' = \frac{1}{\omega} \cdot \frac{2\sqrt{D}}{\log. \frac{1}{2}(T' + U'\sqrt{D})} \cdot \text{lím.} \Sigma \left(\frac{D}{n}\right) \frac{1}{n^{1+\rho}}$$

en la cual h' designa el número de clases de formas de segunda especie, y T', U', la solucion mínima de la ecuacion

$$T'^2 + D\,U'^2 = 4.$$

Recordemos además, como cuestion prévia tambien, y antes de entrar en pormenores, que, duplicando cualquiera solucion (t, u) de la ecuacion $t^2 - D\,u^2 = 1$, se obtiene otra $(t' = 2\,t,\ u' = 2\,u)$, de la ecuacion $t'^2 - D\,u'^2 = 4$; y que, recíprocamente: si tomamos la mitad de una solucion *par* (t', u'), de esta segunda ecuacion, encontramos otra solucion (t, u) de la primera: de lo cual se deduce inmediatamente que $(t' = 2\,T,\ u' = 2\,U)$ será en todo caso la mínima solucion, par, de la ecuacion $t'^2 - D\,u'^2 = 4$. Ahora bien:

Si $D \equiv 1 \pmod 8$, esta última ecuacion admite exclusivamente soluciones *pares;* porque, si cualquiera de los números t', ó u' fuese impar, el otro lo sería tambien; y el primer miembro de aquella entónces divisible por 8, mientras que el segundo es $= 4$: luego efectivamente:

$$T' = 2\,T;\ U' = 2\,U \quad \text{y, por tanto,} \quad \tfrac{1}{2}\,(T' + U'\sqrt{D}) = T + U\sqrt{D};$$

y, como por otra parte es $\omega = 1$, resulta:

$$h' = h \quad \text{cuando} \quad D \equiv 1 \pmod 8.$$

Si $D \equiv 5 \pmod 8$, el resultado ya varia; pues para ciertas determinantes que satisfacen á esta condicion, la solucion mínima (T'', U'') sería par, y para otras impar. En el primer caso, tendremos como antes, $T'' = 2\,T',\ U' = 2\,U;$ y, por consecuencia, como ahora es $\omega = 3$,

$$h' = \tfrac{1}{3}h, \quad \text{cuando} \quad D \equiv 5 \pmod 8 \quad \text{y} \quad T'',\ U' \quad \text{pares.}$$

En el segundo, cuando $T'',\ U'$ sean impares, buscaremos entre todas las soluciones (t', u') que produce la fórmula (158)

$$\frac{t' + u'\sqrt{D}}{2} = \left(\frac{T'' + U'\sqrt{D}}{2}\right)^n$$

para valores positivos de n, la mínima par. Busquemos primeramente la próxima superior, que corresponde al exponente $n = 2$; para este exponente hallamos:

$$t' = \tfrac{1}{2}(T'^2 + D\,U'^2), \qquad u' = T'\,U';$$

y, como u' es evidentemente impar, no nos sirve la solucion hallada. Calculemos la inmediata superior, que corresponde al exponente $n = 3$, y hallaremos:

$$t' = \frac{T'^3 + 3\,DT'\,U'^2}{4} = T'\,\frac{T'^2 + 3\,DU'^2}{4}.$$

De esta expresion última se deduce, por ser

$$T'^2 \equiv U'^2 \equiv 1 \pmod 8, \qquad \text{y} \qquad 3\,D \equiv -1 \pmod 8,$$

que t' es par, y, por consecuencia, lo es tambien u': esto es, podemos como en el caso primero establecer las igualdades, $t' = 2\,T$, $u' = 2\,U$: luego

$$T + U\sqrt{D} = \left(\frac{T' + U'\sqrt{D}}{2}\right)^3$$

$$\log.\ \tfrac{1}{2}(T' + U'\sqrt{D}) = \tfrac{1}{3}\ \log.(T + U\sqrt{D})$$

y, teniendo presente que $\omega = 3$, resulta por último:

$$h' = h, \text{ cuando } D \equiv 5 \pmod 8 \text{ y } T',\ U' \text{ impares.}$$

Inferiores al número 600 existen 75 de la forma $8k+5$. Entre éstos hay 16 (*determinantes*), para los cuales el número de clases de formas primitivas, de primera especie, es tres veces mayor que el de las clases de formas de la segunda especie, que son: 37, 101, 141, 189, 197, 269, 325, 333, 349, 373, 381, 389, 405, 485, 557, 573. Para los 59 restan-

tes, los números de clases de formas de la una, y de la otra especie, son iguales.

174.—*Reduccion del problema que estamos estudiando al caso de una determinante, no divisible por ningun cuadrado.*

En los artículos anteriores hemos visto que el número de clases de formas primitivas, de segunda especie, para una determinante cualquiera, se halla siempre mediante el número de las clases relativas á las formas de primera especie. De lo cual se desprende que el problema, principal objeto de este capítulo, de hallar el número de clases de formas para una determinante conocida, puede desde luego concretarse á encontrar tal número respecto de las formas de primera especie.

Pero no sólo á las formas de la primera especie, sino exclusivamente, además, á aquéllas, cuya determinante D no sea divisible por ningun cuadrado (excepto el 1), puede reducirse todavía el problema que estamos examinando: y de esta nueva restriccion trataremos ahora, para continuar despues con más facilidad nuestro estudio.

Sea D una determinante cualquiera; siempre podremos establecer la igualdad $D = D' S^2$, en la cual S^2 represente el máximo cuadrado, contenido en D; y D', por lo tanto, será un producto de factores primos, desiguales (ó tambien $= -1$), que tendrá igual signo que D. Veamos, pues, cómo el número de clases de formas, para la determinante D, se refiere al número de clases de formas, para la determinante D'. Comparemos primeramente entre sí las dos sumas, relativas á D y D',

$$\Sigma\left(\frac{D}{n}\right)\frac{1}{n^s}. \qquad \Sigma\left(\frac{D'}{n'}\right)\frac{1}{n'^s}.$$

donde, para mayor sencillez, hemos escrito s por $1+\rho$; despues de haberlas distinguido, acentuando la segunda, referente á D', en la cual representará la letra n' todos los números positivos y primos con $2D'$.

Si designamos por q' todos los números primos, positivos, impares, primos con D'; y por q, como anteriormente (164), todos los números primos, positivos é impares, no contenidos en D, tendremos:

$$\Sigma\left(\frac{D}{n}\right)\frac{1}{n^s} = \Pi\frac{1}{1-\left(\frac{D}{q}\right)\frac{1}{q^s}}$$

$$\Sigma\left(\frac{D'}{n'}\right)\frac{1}{n'^s} = \Pi\frac{1}{1-\left(\frac{D'}{q'}\right)\frac{1}{q'^s}}.$$

Ahora bien, evidentemente el conjunto de los números primos q, sólo constituye una parte del conjunto de los números primos q'; porque todo número primo q, que no divida á $D = D' S^2$, tampoco divide á D', y es por lo tanto, uno de los números q': de lo cual se desprende que el conjunto ó sistema de los números q', se compone del relativo á los números q, y de otros números primos, impares, r, no contenidos desde luego en D', pero sí en D, y, de consiguiente, en S, cuya totalidad es sin duda finita. El producto infinito, correspondiente á la determinante D', puede, por consecuencia, descomponerse en otros dos: uno relativo á los factores q, y el otro á los r, del modo siguiente:

$$\Pi\frac{1}{1-\left(\frac{D'}{q'}\right)\frac{1}{q'^s}} = \Pi\frac{1}{1-\left(\frac{D'}{q}\right)\frac{1}{q^s}} \cdot \Pi\frac{1}{1-\left(\frac{D'}{r}\right)\frac{1}{r^s}}$$

y, como de la igualdad $D = D' S^2$ se desprende que

$$\left(\frac{D}{q}\right) = \left(\frac{D' S^2}{q}\right) = \left(\frac{D'}{q}\right),$$

resulta, poniendo las séries por los productos equivalentes:

$$\Sigma\left(\frac{D}{n}\right)\frac{1}{n^s} = \Sigma\left(\frac{D'}{n'}\right)\frac{1}{n'^s} \cdot \Pi\left(1 - \left(\frac{D'}{r}\right)\frac{1}{r^s}\right);$$

y, en consecuencia:

$$\text{lím. } \Sigma\left(\frac{D}{n}\right)\frac{1}{n^{1+\rho}} = \Pi\left(1 - \left(\frac{D'}{r}\right)\frac{1}{r}\right) \text{lím. } \Sigma\left(\frac{D'}{n'}\right)\frac{1}{n'^{1+\rho}},$$

refiriéndose el signo-producto Π á todos los números primos impares r, contenidos en S, pero no en D'.

Establecida así la relacion entre los dos límites análogos, que figuran en las expresiones para los números de clases h y h', relativos á las determinantes D y D', sin haber distinguido el signo de éstas, vamos á examinar ahora separadamente aquellas expresiones, respecto de las formas con determinante negativa, y de las formas con determinante positiva.

Concretándonos, como ya se razonó, á las formas de primera especie, si D' y D, por lo tanto, son *negativas*, tendremos:

$$h = \frac{2\sqrt{-D}}{\pi} \text{lím. } \Sigma\left(\frac{D}{n}\right)\frac{1}{n^{1+\rho}},$$

y, exceptuando únicamente el caso $D' = -1$,

$$h' = \frac{2\sqrt{-D'}}{\pi} \text{lím. } \Sigma\left(\frac{D'}{n'}\right)\frac{1}{n'^{1+\rho}}.$$

Despejando de estas dos ecuaciones los valores de los límites en ellas comprendidos; sustituyéndolos en su relacion antes encontrada; y recordando que $\sqrt{-D}, \sqrt{-D'} = S$, se halla por último, con la única excepcion tambien de $D' = -1$,

$$h = h' \times S \cdot \Pi\left(1 - \left(\frac{D'}{r}\right)\frac{1}{r}\right).$$

En el caso exceptuado, $D' = -1$, en que $\varkappa' = 4$, $h' = 1$; y $D = -S^2$, pero no tambien igual á -1, y, por lo tanto, $S > 1$; el número de clases de formas para la determinante D será:

$$\frac{1}{2} S \Pi \left(1 - \frac{(-1)^{\frac{1}{2}(r-1)}}{r}\right).$$

Relativas á las determinantes *positivas* obtuvimos las siguientes fórmulas:

$$h = \frac{2\sqrt{D}}{\log (T + U\sqrt{D})} \lim. \Sigma \left(\frac{D}{n}\right) \frac{1}{n^{1+\rho}}$$

$$h' = \frac{2\sqrt{D'}}{\log (T' + U'\sqrt{D'})} \lim. \Sigma \left(\frac{D'}{n'}\right) \frac{1}{n'^{1+\rho}},$$

donde T', U' representan los números enteros positivos que verifican la ecuacion $T'^2 - D' U'^2 = 1$. Y, sustituyendo los valores de los límites, deducidos de las dos últimas ecuaciones, en la relacion antes hallada para los mismos, se halla la siguiente:

$$h = h' \frac{\log (T' + U'\sqrt{D'})}{\log (T + U\sqrt{D})} \times S. \Pi \left(1 - \left(\frac{D'}{r}\right) \frac{1}{r}\right).$$

Resta todavía expresar la razon de los logaritmos en forma racional. Para esto reparemos en que toda solucion (t, u) de la ecuacion

$$t^2 - D u^2 = 1 = t^2 - D' S^2 u^2,$$

lo es tambien de esta otra:

$$t'^2 - D' u'^2 = 1:$$

á condicion de que se verifiquen las igualdades

$$t' = t, \qquad u' = S u;$$

ó de que el segundo elemento u', sea divisible por S. Y recíprocamente: si la solucion (t', u') tiene su segundo elemento u', divisible por S, es tambien solucion de la primera. De esto resulta que los dos números

$$t' = T, \qquad u' = S\,U,$$

de los cuales el u' es divisible por S, constituyen la mínima solucion, positiva, de la segunda ecuacion; y podemos, en consecuencia, establecer la igualdad

$$T + S\,U\sqrt{D'} = T + U\sqrt{D} = (T' + U'\sqrt{D'})^{\lambda} :$$

representando λ el mínimo exponente entero, para el cual se hace divisible por S la parte irracional de la potencia correspondiente. Y, si tomamos logaritmos en dicha igualdad, la razon entre los números h y h' se convierte, por fin, en la siguiente:

$$h = h' \times \frac{1}{\lambda} \cdot S\Pi\,(1 - \left(\frac{D'}{r}\right)\frac{1}{r}.$$

Para hallar, si se quiere, el valor de λ, estableceremos, como antes, la igualdad

$$(T' + U'\sqrt{D'})^{\nu} = t'_{\nu} + u'_{\nu}\sqrt{D'};$$

mediante la cual podrá ser conocido el mínimo valor de ν que hace divisible u'_{ν} por cada factor p de los contenidos en S; y al mismo tiempo la máxima potencia de p, contenida en dicho número u'_{ν}.

175.—*Convergencia y continuidad de las séries infinitas que figuran en este asunto.*

—

Circunscrito el problema que estamos estudiando á las determinantes D, que no sean divisibles por ningun cuadrado, diferente de la unidad, procede ahora discutir la série infinita

$$\Sigma\left(\frac{D}{n}\right)\frac{1}{n^{1+\rho}}.$$

cuyo límite vamos á determinar en forma explícita, en el supuesto, ya sentado, de que el valor positivo ρ disminuya indefinidamente.

Mientras el valor de ρ permanezca *positivo*, esta série será siempre convergente; é independiente su suma, por otra parte, del órden en que sus términos se sucedan; mas, para el valor de $\rho = 0$, adquiere la misma otro carácter, entrando en la categoría de aquéllas en las que, tanto la suma de sus términos positivos por sí sola, como la de los negativos tambien aislada, representan un valor infinitamente grande. En las séries de este género, por consecuencia, al tratar de su convergencia, y de su suma que no es, como sabemos, sino el límite á que se aproxima la de sus n primeros términos, en el supuesto de crecer n indefinidamente, debemos preocuparnos del órden en que están estos términos colocados; pues de tal órden depende en primer lugar que la série tenga suma finita, precisamente por la compensacion entónces resultante entre sus dos partes, cada una por sí sola infinita, y compuestas de los términos positivos, y de los negativos, respectivamente.

Toda série infinita del género indicado tendrá, segun lo dicho, diferentes sumas, segun sea la colocacion ú órden de sus términos. Mas supongamos que no sea así la série de que tratamos, sino que, por el contrario, admita para el valor $\rho=0$, uno, finito y determinado; siempre nos restará averiguar si tal valor es tambien el límite á que se aproxima la série en cuestion cuando ρ mengüe indefinidamente: lo cual

equivale á indagar si el valor de la misma da un salto al llegar ρ al límite 0; ó, bien, si por el contrario, varia *continuamente* con ρ, áun el supuesto de $\rho = 0$.

Para desvanecer tales dudas demostraremos, por via de *lema*, la proposicion siguiente:

Si $\alpha_1, \alpha_2, \alpha_3 \ldots\ldots$ *en número infinito, representan constantes, cuya suma*

$$\beta_n = \alpha_1 + \alpha_2 + \alpha_3 + \ldots\ldots + \alpha_n,$$

por grande que sea n, *permanece siempre inferior á otra constante determinada* C, *la série infinita,*

$$\frac{\alpha_1}{1^s} + \frac{\alpha_2}{2^s} + \frac{\alpha_3}{3^s} + \ldots\ldots + \frac{\alpha_m}{m^s},$$

será convergente, y además funcion continua de s, *para todo valor positivo de este exponente* (con la excepcion de $s = 0$).

En efecto, comparemos la série propuesta con esta otra:

$$\beta_1 \left(\frac{1}{1^s} - \frac{1}{2^s}\right) + \beta_2 \left(\frac{1}{2^s} - \frac{1}{3^s}\right) + \beta_3 \left(\frac{1}{3^s} - \frac{1}{4^s}\right) + \ldots\ldots$$

y hallaremos que la diferencia entre las sumas de los n primeros términos de cada una tiene la forma

$$\frac{\beta_n}{(n+1)^s};$$

la cual, como s es positivo, y β_n, por hipótesis, finito, disminuirá indefinidamente cuando n crezca del mismo modo. Esto prueba que, si una de las dos séries fuera convergente, la otra lo seria tambien, y además que una y otra tienen la misma suma. Fijémonos, pues, en la segunda para demostrar que es convergente, primero, y despues, que es una funcion contínua de s.

Sabemos que toda série es convergente cuando la suma de un número cualquiera de términos, siguientes á los n primeros, llega á ser menor en valor absoluto que una cantidad tan pequeña como queramos, creciendo n suficientemente. Segun esto, escribamos la suma de los m términos, siguientes á los n primeros en la série elegida, que será:

$$\beta_{n+1}\left(\frac{1}{(n+1)^s}-\frac{1}{(n+2)^s}\right)+\ldots\ldots+\beta_{n+m}\left(\frac{1}{(n+m)^s}-\frac{1}{(n+m+1)^s}\right)$$

Como, por una parte, las m diferencias

$$\frac{1}{(n+1)^s}-\frac{1}{(n+2)^s},\quad \frac{1}{(n+2)^s}-\frac{1}{(n+3)^s},\ldots\ldots\frac{1}{(n+m)^s}-\frac{1}{(n+m+1)^s},$$

cuya suma total es evidentemente

$$\frac{1}{(n+1)^s}-\frac{1}{(n+m+1)^s},$$

son todas positivas; y, por otra, sus coeficientes

$$\beta_{n+1},\quad \beta_{n+2},\ldots\ldots\beta_{n+m},$$

son numéricamente menores que C; el valor absoluto de la suma de los m términos de la série, antes escritos, será menor tambien que el producto de C por la suma de las m diferencias antes expresadas: esto es, menor que

$$C\left(\frac{1}{(n+1)^s}-\frac{1}{(n+m+1)^s}\right)$$

y, con mayor razon menor que

$$\frac{C}{(n+1)^s} < \frac{C}{n^s}.$$

Luego efectivamente la suma de los m términos, siguientes en la série elegida á los n primeros, si n crece suficientemente, puede llegar á ser menor que cualquiera cantidad dada, por diminuta que la supongamos; y, por consecuencia, dicha série es convergente.

Demostrada la convergencia de la série elegida, vamos á demostrar ahora que su valor varía contínuamente con s, considerando para ello todos los valores positivos de s, mayores que uno determinado σ; porque, por muy pequeño que supongamos á s, no siendo $= 0$, siempre existirá otro número tambien positivo, aún más pequeño, σ: de lo cual se desprende que la demostracion, al parecer limitada á ciertos valores de s, se refiere realmente á todos los valores positivos de este exponente (el 0 exclusive).

Dicho esto, descompongamos la série propuesta en dos partes: una que comprenda sus n primeros términos, y la otra los restantes. La primera, esto es, la suma de los n primeros términos, segun hemos probado, se aproxima á un límite finito y determinado; y es, de consiguiente, una funcion contínua de s; la segunda sabemos de seguro que es

$$< \frac{C}{n^s} \quad \text{y, con mas razon,} < \frac{C}{n^\sigma}:$$

y menor, por consecuencia, que toda cantidad, por pequeña que sea, elegido n suficientemente grande, sin que en esto influyan, por otra parte, los valores de $s > \sigma$. Ahora bien, siendo contínua la primera parte, si existe discontinuidad en la série entera, es claro que debe depender de la segunda; pero esta segunda parte para todos los valores considerados de s, es menor en absoluto que $C n^{-\sigma}$; y menor que $2 C n^{-\sigma}$, por lo tanto, la variacion ó salto que en el valor de la série total pudiera resultar por el trascurso de un valor determinado de s; y, como tal variacion ó salto puede hacerse tan pequeño como queramos, con solo tomar n suficientemente grande, resulta que tal salto, signifi-

cativo, no puede existir realmente, y, en consecuencia, la série de que se trata es una funcion contínua de s.

Apliquemos ahora los principios demostrados á la série infinita

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n^{1+\rho}},$$

cuyos términos supondremos desde luego *ordenados* de modo que vaya n *creciendo constantemente*. Con esta condicion se comprende bien pronto que la última série es un caso particular de la estudiada en el lema precedente. En efecto, hagamos

$$\alpha_m = \left(\frac{D}{m}\right), \text{ ó } = 0,$$

segun que m sea primo con $2D$, ó no lo sea. Si m recorre un sistema completo de restos (mod. $4D$), la suma de los correspondientes valores de α_m será siempre $= 0$; pues, en primer lugar, los coeficientes α_m, correspondientes á los valores de m que no sean primos con $2D$, son desde luego $= 0$; y los coeficientes α_m, correspondientes á los valores de m primos con $2D$, esto es, á los números n, son por mitad iguales á $+1$, y á -1. Y, por consecuencia, la suma de un número cualquiera de coeficientes sucesivos α_m, será siempre inferior á la cantidad finita $(\pm 2D)$: condicion indispensable, que exijimos en el lema, para que la série allí establecida fuera convergente. Así, la série, ordenada como se ha dicho,

$$\Sigma \frac{\alpha_m}{m^s} = \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s},$$

será convergente y funcion contínua de s, para todo valor positivo de este exponente; y, en conclusion, cuando ρ disminuya indefinidamente,

$$\lim. \Sigma \left(\frac{D}{n}\right) \frac{1}{n^{1+\rho}} = \Sigma \left(\frac{D}{n}\right) \frac{1}{n}:$$

á condicion de que los términos de esta série, repetimos, estén *ordenados* de tal modo que n *vaya creciendo constantemente.*

SUMA DE ESTA SÉRIE EN LOS CUATRO CASOS QUE PUEDEN OCURRIR.

En la sumacion de la série

$$N = \Sigma \left(\frac{D}{n}\right) \frac{1}{n}$$

distinguiremos los mismos cuatro casos principales que en el artículo (121), á saber:

$$D = \pm P \equiv 1 \pmod 4, \delta = +1, \quad \varepsilon = +1$$

$$D = \pm P \equiv 3 \pmod 4, \delta = -1, \quad \varepsilon = +1$$

$$D = \pm 2P \equiv 2 \pmod 8, \delta = +1, \quad \varepsilon = -1$$

$$D = \pm 2P \equiv 6 \pmod 8, \delta = -1, \quad \varepsilon = -1,$$

en todos los cuales, segun la ley de reciprocidad generalizada (118), se verificará la igualdad simbólica

$$\left(\frac{D}{n}\right) = \delta^{\frac{1}{2}(n-1)} \varepsilon^{\frac{1}{8}(n^2-1)} \left(\frac{n}{P}\right),$$

(donde n representa todos los números positivos y primos con $2D$, y las letras P, δ, ε lo mismo que en el artículo citado); y tambien, en consecuencia, esta otra

$$\left(\frac{D}{n}\right) = \left(\frac{D}{\nu}\right)$$

siempre que sea

$$n \equiv \nu \pmod{8\,P}.$$

176.—*Suma en el primero.*

Conforme acabamos de expresar, la determinante D, en este caso, tiene la forma $4n+1$, ó bien es

$$D = \pm P \equiv 1 \pmod{4};$$

y, por tanto: $\left(\frac{D}{n}\right) = \left(\frac{n}{P}\right)$, designando P el valor absoluto de la determinante D; y, de consiguiente, un número positivo *impar*, no divisible por ningun cuadrado, mayor que 1.

a-) La série para este caso será

$$N = \Sigma \left(\frac{n}{P}\right)\frac{1}{n},$$

en la cual n representa todos los números positivos *impares*, y primos con P. Y vamos á demostrar primeramente que tal série puede, para su sumacion, referirse á esta otra

$$M = \Sigma \left(\frac{m}{P}\right)\frac{1}{m},$$

donde la letra m exprese *todos* los números positivos, primos con P, no sólo impares, sino tambien *pares;* pero crecientes siempre, conforme lo exije su convergencia. Para esto observaremos que la série infinita

$$\left(\frac{2^r}{P}\right)\frac{1}{2^r}.$$

en el supuesto de que r reciba sucesivamente todos los valores 0, 1, 2, 3, ... de la natural ó entera, es una progresion geométrica cuyo primer término es la unidad, su razon $\left(\frac{2}{P}\right)\frac{1}{2}$, y su suma, por consecuencia:

$$\frac{1}{1-\left(\frac{2}{P}\right)\frac{1}{2}} = \Sigma\left(\frac{2^r}{P}\right)\frac{1}{2^r}.$$

Multiplicando por esta igualdad ordenadamente la anterior

$$N = \Sigma\left(\frac{n}{P}\right)\frac{1}{n},$$

resulta la siguiente:

$$\frac{N}{1-\left(\frac{2}{P}\right)\frac{1}{2}} = \Sigma\left(\frac{n}{P}\right)\frac{1}{n} \times \Sigma\left(\frac{2^r}{P}\right)\frac{1}{2^r} = \Sigma\left(\frac{2^r.n}{P}\right)\frac{1}{2^r.n}:$$

donde se ve claro que los términos, en el producto de su segundo miembro, son de la forma

$$\left(\frac{2^r.n}{P}\right)\frac{1}{2^r.n},$$

representando los comprendidos en la $2^r.n$, números primos con P, sin distincion de pares é impares; y, como todo número m, primo con P, puede de un solo modo ser expresado por la forma $2^r.n$, los valores de ésta serán todos diferentes, y coincidirán, por consecuencia, con los números m. Haciendo, pues, $2^r.n = m$ en la última igualdad, resulta la que buscábamos:

$$N = \left(1-\left(\frac{2}{P}\right)\frac{1}{2}\right)M.$$

Aún podríamos añadir que m representa todos los números positivos, sin excepcion, con tal de suponer $\left(\frac{m}{P}\right) = 0$, siempre que m y P tengan algun factor comun.

b-) Vamos á efectuar ahora la sumacion de la série infinita M. Recordaremos para esto que, siendo m un número cualquiera, entero y positivo, tenemos:

$$\frac{1}{m} = \int_0^1 x^{m-1}\, dx:$$

luego

$$\Sigma\left(\frac{m}{P}\right)\frac{1}{m} = \Sigma\left(\frac{m}{P}\right)\int_0^1 x^{m-1}\, dx \cdot \quad \Sigma\left(\frac{m}{P}\right)\int_0^1 \frac{dx}{x}\cdot x^m$$

Si recordamos que el símbolo de Jacobi $\left(\frac{m}{P}\right)$ tiene el mismo valor para todos los números congruentes (mod. P); y que todos estos números se hallan agrupados en clases, cuyos representantes son los restos de P.

$$0,\ 1,\ 2,\ 3,\ \ldots\ldots\ (P-1):$$

y admitimos que la letra μ designe cada uno de todos estos restos, y la funcion $f(x)$ el conjunto de los valores correspondientes á los mismos (y los solos diferentes entre sí) de la suma

$$\Sigma\left(\frac{\mu}{P}\right)x^{\mu} = f(x);$$

la de los términos de la série en cuestion, arriba escrita, en los cuales sea $m < KP$, tomará la forma:

$$\int_0^1 \frac{dx}{x} f(x)\,\frac{1-x^{KP}}{1-x^{P}}.$$

Ahora bien, significando μ un sistema completo de restos (módulo P), será (121)

$$\Sigma\left(\frac{\mu}{P}\right) = 0, \text{ y, de consiguiente, } f(1) = \Sigma\left(\frac{\mu}{P}\right) = 0:$$

lo cual prueba que la funcion $f(x)$ es divisible por $x(x-1)$, y que la fraccion

$$\frac{1}{x} \cdot \frac{f(x)}{1-x^P} = F(x),$$

dentro de los límites reales de integracion, $0 \leq x \leq 1$, tiene, por lo tanto, valores finitos. Sustituyendo, pues, esta última expresion en la integral anterior, resulta la siguiente:

$$\int_0^1 F(x)\left\{1 - x^{KP}\right\} dx = \int_0^1 F(x)\,dx - \int_0^1 F(x)\,x^{KP}\,dx;$$

y, como el segundo término ó sustraendo de esta diferencia, creciendo K indefinidamente, se hace infinitamente pequeño, la integracion que debemos efectuar queda reducida á la de la expresion

$$\int_0^1 F(x)\,dx = \int_0^1 \frac{dx}{x} \cdot \frac{f(x)}{1-x^P}$$

cuyo valor, despreciado el término infinitamente pequeño antes mencionado, representa efectivamente el de la suma

$$\Sigma\left(\frac{m}{P}\right)\frac{1}{m}.$$

Conocido es el método para integrar una fraccion racional como la que ahora se nos ofrece: consiste en descomponerla en fracciones parciales cuyos denominadores sean los factores simples del denominador de la propuesta. Debemos, por consecuencia, hallar ante todo estos fac-

tores simples. Para ello recordaremos que el denominador de la fraccion actual, igualado á cero, constituye la ecuacion binomia

$$x^P - 1 = 0,$$

cuyas raices todas se hallan compendiadas (122) en la forma

$$\cos. \frac{2\alpha\pi}{P} + i \operatorname{sen}. \frac{2\alpha\pi}{P} = e^{\frac{2\alpha\pi i}{P}} = \theta^\alpha,$$

á condicion de que α reciba los valores del sistema completo de restos (mod. P)

$$0,\ 1,\ 2 \ldots\ldots (P-1).$$

Segun esto, podremos escribir la ecuacion

$$x^P - 1 = \Pi (x - \theta^\alpha),$$

donde se refiere el signo-producto á todas las raices de la ecuacion binomia consabida, y tambien (*) esta otra:

$$\frac{1}{x} \cdot \frac{f(x)}{1 - x^P} = -\frac{1}{P} \Sigma \frac{f(\theta^\alpha)}{x - \theta^\alpha}$$

en la cual se refiere el signo-suma á los valores ya dichos que puede recibir la letra α. Mas la funcion f, segun la definicion antes establecida, correspondiente al valor de $x = \theta^\alpha$ es evidentemente:

$$f(\theta^\alpha) = \Sigma \left(\frac{\mu}{P}\right) e^{\mu \frac{2\alpha\pi i}{P}}$$

y esta suma (Apénd. IV—6)

(*) Puede consultar el lector, si lo cree necesario, el *Algebra superior*, ya citada, de Serret, 3.ª edicion, tomo I, pág. 487.

$$= \left(\frac{\alpha}{P}\right)\sqrt{P}\,.\,i^{\frac{1}{4}(P-1)^2}$$

en la cual deberá tomarse la raiz de P *positivamente*, y hacer

$$\left(\frac{\alpha}{P}\right) = 0,$$

siempre que α no sea primo con P. Luego, sustituyendo este valor de $f(\vartheta^\alpha)$ en la expresion de arriba, obtendremos el resultado:

$$\frac{1}{x}\cdot\frac{f(x)}{1-x^P} = -\frac{i^{\frac{1}{4}(P-1)^2}}{\sqrt{P}}\,\Sigma\,\frac{\left(\frac{\alpha}{P}\right)}{x-\vartheta^\alpha},$$

refiriéndose la sumacion á todos los valores de α, *primos* con P y menores que este número.

Las $\psi(P)$ integraciones que debemos efectuar, por consecuencia, relativas á cada una de las fracciones parciales que se desprenden de la descomposicion atrás indicada, se hallan comprendidas en la fórmula conocida

$$\int\frac{dx}{x-(a+bi)} = \int\frac{(x-a+bi)\,dx}{(x-a)^2+b^2} = \int\frac{(x-\alpha)\,dx}{(x-a)^2+b^2} + \int\frac{b\,i\,dx}{(x-a)^2+b^2}$$

$$= \frac{1}{2}\log\left[(x-a)^2+b^2\right] + i\left(\text{arc. } tg = \frac{x-a}{b}\right)$$

ó bien, haciendo

$$a+bi = \cos\delta + i\,\text{sen}\,\delta = e^{\delta i}$$

$$\int\frac{dx}{x-e^{\delta i}} = \frac{1}{2}\log\left(x^2-2x\cos\delta+1\right) + i\left(\text{arc. } tg = \frac{x-\cos\delta}{\text{sen}\,\delta}\right).$$

De la cual, cuando $0 < \delta < 2\pi$, se deduce la definida:

$$\int_0^1 \frac{dx}{x - e^{\delta i}} = \log(2 \operatorname{sen} \tfrac{1}{2}\delta) + i\{\text{arc. } tg = tg \cdot \tfrac{1}{2}\delta + \text{arc. } tg = \operatorname{cotg} \delta\}$$

con tal que los dos arcos, inclusos en el paréntesis, se tomen entre $+\frac{1}{2}\pi$ y $-\frac{1}{2}\pi$; y, si δ se toma entre 0 y π, ó entre π y 2π, la siguiente:

$$\int_0^1 \frac{dx}{x - e^{\delta i}} = \log\left(2 \operatorname{sen} \tfrac{1}{2}\delta\right) + i\left(\tfrac{1}{2}\pi - \tfrac{1}{2}\delta\right).$$

Aplicando esta última fórmula se halla con facilidad:

$$\int_0^1 \frac{dx}{x - 1^{\alpha}} = \log\left(2 \operatorname{sen} \frac{\alpha\pi}{P}\right) + i\left(\frac{\pi}{2} - \frac{\alpha\pi}{P}\right),$$

y, por consecuencia:

$$\Sigma\left(\frac{m}{P}\right)\frac{1}{m} = -\frac{i^{\frac{1}{1}(P-1)^2}}{\sqrt{P}} \Sigma\left(\frac{\alpha}{P}\right)\left\{\log\left(2 \operatorname{sen} \frac{\alpha\pi}{P}\right) + i\left(\frac{\pi}{2} - \frac{\alpha\pi}{P}\right)\right\}$$

refiriéndose el signo-suma del segundo miembro á todos los $\varphi(P)$ valores de α. Y, como de ser esto así, resulta

$$\Sigma\left(\frac{\alpha}{P}\right) = 0,$$

podremos, de consiguiente, despreciar todos los términos independientes de α, tales como $\log 2$ y $\frac{1}{2}\pi i$: con lo cual se reduce la última ecuacion á la que sigue:

$$\Sigma\left(\frac{m}{P}\right)\frac{1}{m} = -\frac{i^{\frac{1}{4}(P-1)^2}}{\sqrt{P}}\Sigma\left(\frac{\alpha}{P}\right)\left\{\log\operatorname{sen}\frac{\alpha\pi}{P} - \frac{\alpha\pi i}{P}\right\}$$

Todavía puede simplificarse más este resultado si consideramos separadamente los dos casos $P \equiv 1 \pmod 4$ y $P \equiv 3 \pmod 4$. Efectivamente: en el primero es

$$i^{\frac{1}{4}(P-1)^2} = 1,$$

y, por tanto, como el primer miembro de la ecuacion última es *real*, tendremos:

$$\Sigma\left(\frac{m}{P}\right)\frac{1}{m} = -\frac{1}{\sqrt{P}}\Sigma\left(\frac{\alpha}{P}\right)\log\operatorname{sen}\frac{\alpha\pi}{P}$$

$$\Sigma\left(\frac{\alpha}{P}\right)\alpha = 0;$$

en el segundo, es

$$i^{\frac{1}{4}(P-1)^2} = i$$

y, en consecuencia:

$$\Sigma\left(\frac{m}{P}\right)\frac{1}{m} = -\frac{\pi}{P\sqrt{P}}\Sigma\left(\frac{\alpha}{P}\right)\alpha$$

$$\Sigma\left(\frac{\alpha}{P}\right)\log\operatorname{sen}\frac{\alpha\pi}{P} = 0.$$

Estas dos simplificaciones pueden aún efectuarse de este otro modo. Teniendo en cuenta que la expresion complementaria $(P - \alpha)$ adquiere los mismos valores que α, aunque en otro órden, será:

$$\Sigma\left(\frac{\alpha}{P}\right)\alpha = \Sigma\left(\frac{P-\alpha}{P}\right)(P-\alpha) = -\Sigma\left(\frac{-\alpha}{P}\right)\alpha$$

$$\Sigma\left(\frac{\alpha}{P}\right)\log\operatorname{sen}\frac{\alpha\,\pi}{P} = \Sigma\left(\frac{P-\alpha}{P}\right)\log\operatorname{sen}\frac{(P-\alpha)\,\pi}{P} =$$

$$= \Sigma\left(\frac{-\alpha}{P}\right)\log\operatorname{sen}\frac{\alpha\,\pi}{P}.$$

Ahora bien: si $P \equiv 1 \pmod 4$,

$$\Sigma\left(\frac{\alpha}{P}\right)\alpha = -\Sigma\left(\frac{\alpha}{P}\right)\alpha = 0:$$

si, por el contrario, $P \equiv 3 \pmod 4$,

$$\Sigma\left(\frac{\alpha}{P}\right)\log\operatorname{sen}\frac{\alpha\,\pi}{P} = -\Sigma\left(\frac{\alpha}{P}\right)\log\operatorname{sen}\frac{\alpha\,\pi}{P} = 0.$$

c—) Hallado ya bajo forma definida el límite de la suma

$$\Sigma\left(\frac{D}{n}\right)\frac{1}{n} = \left\{1 - \left(\frac{2}{P}\right)\frac{1}{2}\right\}\Sigma\left(\frac{m}{P}\right)\frac{1}{m}$$

para el caso que estamos discutiendo, relativo á una determinante $D = \pm P \equiv 1 \pmod 4$, no divisible por ningun cuadrado, vamos á buscar ahora, en forma finita tambien, el valor del número h, que expresa, como sabemos, el de las formas primitivas de primera especie, para la mencionada determinante D. En esta investigacion distinguiremos, segun costumbre, las determinantes negativas de las positivas.

Determinantes negativas.—Para la determinante $D = -P$, y, por consecuencia, $P \equiv 3 \pmod 4$ obtuvimos (171) la expresion del número

$$h = \frac{2\sqrt{-D}}{\pi} \Sigma \left(\frac{D}{n}\right) \frac{1}{n};$$

y, como en este caso es, segun acabamos de probar,

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n} = \left\{1 - \left(\frac{2}{P}\right) \frac{1}{2}\right\} \Sigma \left(\frac{m}{P}\right) \frac{1}{m} =$$

$$= - \left\{1 - \left(\frac{2}{P}\right) \frac{1}{2}\right\} \frac{\pi}{P\sqrt{P}} \Sigma \left(\frac{\alpha}{P}\right) \alpha,$$

resulta:

$$h = - \frac{1}{P} \left\{2 - \left(\frac{2}{P}\right)\right\} \Sigma \left(\frac{\alpha}{P}\right) \alpha,$$

significando α todos los enteros positivos, primos con P, y menores que este número. Esta última expresion de h puede simplificarse mediante las siguientes consideraciones. Si representamos por α' los números α, menores que $\frac{1}{2}P$, los complementarios $(P - \alpha')$ coincidirán con los números α, mayores que $\frac{1}{2}P$; y, por consecuencia:

$$\Sigma \left(\frac{\alpha}{P}\right) \alpha = \Sigma \left(\frac{\alpha'}{P}\right) \alpha' + \Sigma \left(\frac{P - \alpha'}{P}\right) (P - \alpha');$$

y, como ahora es $P \equiv 3 \pmod 4$, y de consiguiente

$$\left(\frac{P - \alpha'}{P}\right) = \left(\frac{-1}{P}\right) \left(\frac{\alpha'}{P}\right) = - \left(\frac{\alpha'}{P}\right),$$

será:

$$\Sigma \left(\frac{\alpha}{P}\right) \alpha = 2 \Sigma \left(\frac{\alpha'}{P}\right) \alpha' - P \Sigma \left(\frac{\alpha'}{P}\right).$$

Por otra parte es tambien evidente que los números $2\alpha'$ y $(P-2\alpha')$ constituyen por completo la série de los números α, y, por lo tanto:

$$\Sigma\left(\frac{\alpha}{P}\right)\alpha = \Sigma\left(\frac{2\alpha'}{P}\right)2\alpha' + \Sigma\left(\frac{P-2\alpha'}{P}\right)\left(P-2\alpha'\right).$$

ó, despues de sencillas reducciones (118):

$$\left(\frac{2}{P}\right)\Sigma\left(\frac{\alpha}{P}\right)\alpha = 4\Sigma\left(\frac{\alpha'}{P}\right)\alpha' - P\Sigma\left(\frac{\alpha'}{P}\right).$$

Restando esta ecuacion de la antepenúltima, multiplicada por 2, se obtiene la siguiente:

$$\left\{2-\left(\frac{2}{P}\right)\right\}\Sigma\left(\frac{\alpha}{P}\right)\alpha = -P\Sigma\left(\frac{\alpha'}{P}\right),$$

y por medio de esta se convierte la expresion de h en la sencillísima:

$$h = \Sigma\left(\frac{\alpha'}{P}\right).$$

Traduciendo este resultado al lenguaje vulgar, podemos decir en resúmen:

Si P es un número positivo, de la forma $4n+3$, no divisible por ningun cuadrado, y α' representa todos los números primos con P y menores que $\frac{1}{2}P$, el número h, que expresa cuántas clases existen de formas de la primera especie para la determinante $D=-P$, se hallará restando del conjunto de los números α', para los cuales se verifique la condicion

$$\left(\frac{\alpha'}{P}\right) = +1,$$

el conjunto de los restantes.

En el supuesto de ser P un número primo absoluto, la ley anterior se modifica del modo siguiente:

Si el valor absoluto p, de la determinante negativa $D=-p$, es un número primo, de la forma $4n+3$, el número h será igual al exceso del número de restos de p sobre el de no-restos: comprendidos unos y otros entre los límites 0 y $\frac{1}{2}p$.

Sea, por ejemplo, la determinante $D=-11$: entre los números $1, 2, 3, 4, 5$, menores que $\frac{1}{2}11$, existen cuatro restos cuadráticos de 11, á saber: 1, 3, 4, 5; y el no-resto 2; el exceso del número de los primeros sobre el del segundo es $4-1=3$. Y, en efecto: 3 es el número de las formas reducidas, de primera especie, no equivalentes, que existen para la determinante $D=-11$: siendo tales formas $(1, 0, 11)$, $(3, 1, 4)$, y $(3, -1, 4)$.

Como de pasada haremos notar que, debiendo ser h un número positivo, y nunca cero, *el conjunto de los números α', para los cuales*

$$\left(\frac{\alpha'}{P}\right)=+1,$$

será siempre mayor que el de los números α', para los cuales

$$\left(\frac{\alpha'}{P}\right)=-1.$$

Determinantes positivas.—Para la determinante positiva $D=+P$, y por consecuencia, $P\equiv 1 \pmod 4$, obtuvimos la expresion (173)

$$h=\frac{2\sqrt{D}}{\log\left(T+U\sqrt{D}\right)}\Sigma\left(\frac{D}{n}\right)\frac{1}{n};$$

y, como en este caso es

$$\Sigma\left(\frac{D}{n}\right)\frac{1}{n}=\left\{1-\left(\frac{2}{P}\right)\frac{1}{2}\right\}\Sigma\left(\frac{m}{P}\right)\frac{1}{m}=$$

$$=-\frac{1-\left(\frac{2}{P}\right)\frac{1}{2}}{\sqrt{P}}\Sigma\left(\frac{\alpha}{P}\right)\log\operatorname{sen}\frac{\alpha\pi}{P}.$$

resulta:

$$h = -\frac{2 - \left(\frac{2}{P}\right)}{\log (T + U\sqrt{P})} \Sigma \left(\frac{\alpha}{P}\right) \log \operatorname{sen} \frac{\alpha \pi}{P}.$$

Designando por a, ó por b, aquellos de los números α, para los cuales sea

$$\left(\frac{\alpha}{P}\right) = +1, \quad \text{ó} \quad = -1,$$

respectivamente, la última ecuacion puede escribirse bajo la forma:

$$h = \frac{2 - \left(\frac{2}{P}\right)}{\log (T + U\sqrt{P})} \log \frac{\Pi \operatorname{sen} \frac{b\pi}{P}}{\Pi \operatorname{sen} \frac{a\pi}{P}},$$

refiriéndose el signo producto en el numerador á todos los no-restos b, y á todos los restos a, en el denominador; y representando T, U los mínimos enteros, positivos, que satisfacen á la ecuacion pelliana

$$T^2 - PU^2 = 1.$$

177.—*Estudio de los casos restantes.*

Examinado el caso primero, en que la determinante tiene la forma $D \equiv 1 \pmod 4$, vamos ahora á estudiar la cuestion de un modo general; y para esto á determinar préviamente la série

$$N = \Sigma \left(\frac{D}{n}\right) \frac{1}{n}.$$

en la cual n significa todos los enteros positivos, y sucesivamente crecientes, que sean primos con $2D$.

Si establecemos, pues, como antes, las ecuaciones

$$\frac{1}{n} = \int_0^1 x^{-1}\, dx$$

$$f(x) = \Sigma \left(\frac{D}{\nu}\right) x^{\nu},$$

en las que ν representa todos los números, entre los n ya definidos, que sean menores que $8P$, y recordamos (176) que $f(1) = 0$; en el supuesto de que el módulo de la variable x permanezca menor que la unidad para que la integral definida entre los límites 0 y 1 tenga valores finitos, será (176):

$$N = \int_0^1 \frac{dx}{x} \cdot \frac{f(x)}{1 - x^{8P}} = -\frac{1}{8P} \int_0^1 \Sigma \frac{f(\omega)\, dx}{x - \omega},$$

á condicion de que ω exprese todas las raices de la ecuacion binomia

$$\omega^{8P} = 1.$$

Lo que ante todo importa conocer ahora es el valor $f(\omega)$, que toma la funcion $f(x)$, para $x = \omega$. Con este propósito recordaremos que las raices ω son (101) los vários productos de las correspondientes á las dos ecuaciones parciales

$$\omega^8 = 1 \quad \text{y} \quad \omega^P = 1,$$

compendiadas respectivamente en las fórmulas:

$$\cos. \frac{2r\pi}{8} + i \operatorname{sen}. \frac{2r\pi}{8} = e^{\frac{r\pi i}{4}} \quad \text{y} \quad \cos. \frac{2s\pi}{P} + i \operatorname{sen}. \frac{2s\pi}{P} = e^{\frac{2s\pi \cdot}{P}}.$$

bajo el supuesto de que r y s recorran, cada una por su parte, un sistema completo de restos, segun los módulos 8 y P. Por consecuencia, si hacemos

$$j = e^{\frac{\pi i}{4}} = \frac{1+i}{\sqrt{2}} \quad (122\text{-}a), \qquad \theta = e^{\frac{2\pi i}{P}},$$

las raices ω quedarán bien expresadas por la fórmula

$$\omega = j^r \theta^s;$$

y con esto será tambien:

$$f(\omega) = \Sigma\left(\frac{D}{\nu}\right)\omega^\nu = \Sigma\,\delta^{\frac{1}{2}(\nu-1)}\,\varepsilon^{\frac{1}{8}(\nu^2-1)}\left(\frac{\nu}{P}\right) j^{\nu r}\,\theta^{\nu s}.$$

Designando por μ los restos mínimos positivos de $\nu \pmod 8$, y por m los de $\nu \pmod P$, es claro que los restos μ serán los cuatro números $1, 3, 5, 7$; y los restos m los $\varphi(P)$ números primos con P; y, como á cada par (μ, m), de tales restos, corresponde (71) un solo número determinado ν, la última ecuacion (*Ap. IV*—6) se convierte en la siguiente:

$$f(\omega) = \Sigma\,\delta^{\frac{1}{2}(\mu-1)}\,\varepsilon^{\frac{1}{8}(\mu^2-1)}\,j^{\mu r}\,\Sigma\left(\frac{m}{P}\right)\theta^{ms} \qquad (*)$$

$$= j^r\left(1+\delta i^{3r}\right)\left(1+\varepsilon(-1)^r\right)\left(\frac{s}{P}\right) i^{\frac{1}{4}(P-1)^2}\sqrt{P},$$

*) La suma primera es:

$$\delta^{0}\varepsilon^{0} j^{r} + \delta\varepsilon j^{3r} + \delta^{2}\varepsilon^{3} j^{5r} + \delta^{3}\varepsilon^{6} j^{7r} = j^r\left(\delta^{0}\varepsilon^{0} + \delta\varepsilon j^{2r} + \delta^{2}\varepsilon^{3} j^{4r} + \delta^{3}\varepsilon^{6} j^{6r}\right);$$

pero $j^2 = i$, y, de consiguiente, $j^{2r} = i^r = i^{5r}$; $j^{4r} = i^{2r} = (-1)^r$; $j^{6r} = i^{3r}$: y

donde $\sqrt{P}$ se toma positivamente) y el símbolo de Jacobi tiene el valor *cero*, siempre que s no sea primo con P. Y, si por abreviar, establecemos la igualdad

$$\psi(r) = \int_0^1 \Sigma \left(\frac{s}{P}\right) \frac{dx}{x - j^r \theta^s};$$

en la que puede recorrer la letra s todos los números incongruentes (mod. P) y primos con este módulo, la expresion de la série N será por último:

$$N = -\frac{i^{-\frac{1}{4}(P-1)^2}}{8\sqrt{P}} \Sigma j^r \left(1 + \delta i^{3r}\right)\left(1 + \varepsilon(-1)^r\right) \psi(r).$$

donde r representa un sistema completo de restos (mod. 8). Dando, pues, á r estos valores, á saber, 0, 1, 2, ... 7, se obtienen para los cuatro casos en un principio distinguidos, los resultados respectivos siguientes:

I. $D = \pm P \equiv 1 \pmod 4$; $\delta = +1$, $\varepsilon = +1$;

$$N \cdot 2\sqrt{P} = -i^{\frac{1}{4}(P-1)^2}\left\{\psi(0) - \psi(4)\right\}$$

II. $D = \pm P \equiv 3 \pmod 4$; $\delta = -1$, $\varepsilon = +1$:

$$N \cdot 2\sqrt{P} = -i \cdot i^{\frac{1}{4}(P-1)^2}\left\{\psi(2) - \psi(6)\right\}$$

---

las potencias pares de δ y ε son la unidad positiva: luego la suma en cuestion será:

$$j^r\left(1 + \delta\varepsilon i^{2r} \cdot i^{3r} + \varepsilon(-1)^r + \delta i^{3r}\right) = j^r\left(1 + \delta i^{3r}\right)\left(1 + \varepsilon(-1)^r\right).$$

La otra suma no ofrece dificultad ninguna; pues es la misma del Apéndice citado en el texto.

III. $D = \pm 2P \equiv 2 \pmod 8$; $\delta = +1$, $\varepsilon = -1$

$$N \cdot 2\sqrt{2P} = -i^{\frac{1}{4}(P-1)^2}\left\{\psi(1) - \psi(3) - \psi(5) + \psi(7)\right\}$$

IV. $D = \pm 2P \equiv 6 \pmod 8$; $\delta = -1$, $\varepsilon = -1$

$$N \cdot 2\sqrt{2P} = -i \cdot i^{\frac{1}{4}(P-1)^2}\left\{\psi(1) + \psi(3) - \psi(5) - \psi(7)\right\}$$

Estas fórmulas comprenden tambien el caso $P = 1$, esto es, se verifican para las determinantes $D = -1$, $D = +2$, $D = -2$. En efecto, aplicando á la integral referente á este caso,

$$\psi(r) = \int_0^1 \frac{dx}{x - j^r},$$

la fórmula general, antes hallada, se obtiene la siguiente:

$$\int_0^1 \frac{dx}{x - j^r} = \log.\left(2 \operatorname{sen.} \frac{r\pi}{8}\right) + \frac{1}{2}\left(\pi - \frac{r\pi}{4}\right)i;$$

y, dando en ésta sucesivamente á r los valores numéricos que figuran en las fórmulas II, III, IV, resulta:

$$D = -1, \quad N = \frac{\pi}{4}$$

$$D = +2, \quad N = \frac{\log.(1+\sqrt{2})}{\sqrt{2}} \qquad (1)$$

$$D = -2, \quad N = \frac{\pi}{2\sqrt{2}}$$

siendo $\sqrt{2}$ siempre positiva. Excluyendo desde ahora este caso $P=1$, y designando por m los restos mínimos positivos (mód. $8P$) del número $(Pr+8s)$, para lo cual es indispensable (72) que se verifiquen las relaciones

$$m \equiv Pr \,(\text{mod. } 8), \quad m \equiv 8s \,(\text{mod. } P), \quad 0 < m < 8P,$$

será:

$$\int_0^1 \frac{dx}{x - j^{r} \theta^{s}} = \log.\left(2 \text{ sen. } \frac{m\pi}{8P}\right) + \left(\frac{\pi}{2} - \frac{m\pi}{8P}\right) i,$$

y, en consecuencia:

$$\dot{\psi}(r) = \left(\frac{2}{P}\right) \Sigma \left(\frac{m}{P}\right) \left\{ \log.\left(2 \text{ sen. } \frac{m\pi}{8P}\right) + \left(\frac{\pi}{2} - \frac{m\pi}{8P}\right) i \right\};$$

donde m designa los $\dot{\varphi}(P)$ números positivos, primos con P, menores que $8P$, y al mismo tiempo $\equiv Pr \,(\text{mod. } 8)$. Mas estos números m son tambien incongruentes, segun el módulo P: por lo cual

$$\Sigma \left(\frac{m}{P}\right) = 0,$$

y pueden, de consiguiente, suprimirse en la última expresion todos los términos independientes de m, y quedar entónces reducida á la forma:

$$\dot{\psi}(r) = \left(\frac{2}{P}\right) \Sigma \left(\frac{m}{P}\right) \left(\log. \text{ sen. } \frac{m\pi}{8P} - \frac{m\pi i}{8P}\right) \tag{2}$$

$$m \equiv Pr \,(\text{mod. } 8), \qquad 0 < m < 8P.$$

Con esto la série infinita N se convierte en una suma de un número finito de términos en todos los casos que pueden ocurrir; mas todavía dicha série es susceptible de importantes modificaciones, fundadas en algunas propiedades de las ocho expresiones para $\dot{\psi}(r)$, que vamos

á deducir de la definicion antes establecida para tal funcion. Esta definicion es, como sabemos:

$$\psi(r) = \int_0^1 \Sigma\left(\frac{s}{P}\right) \frac{dx}{x - j^r \vartheta^s};$$

la cual, si hacemos por abreviar

$$F(x) = \Pi(x - \vartheta^s)^{\left(\frac{s}{P}\right)} = \frac{\Pi(x - \vartheta^a)}{\Pi(x - \vartheta^b)} \qquad (3)$$

donde las letras a y b tienen la significacion que les dimos (121), se convierte en la siguiente:

$$\psi(r) = \int_0^1 d \log. F(x j^{-r});$$

con tal que el módulo de la variable x permanezca siempre <1, en el intervalo de 0 á 1; ó bien, en esta otra:

$$\psi(r) = \int_0^{j^{-r}} d \log F(x);$$

si, admitida la representacion geométrica de las cantidades complejas por puntos en un plano, el punto x, en el intervalo de 0 hasta j^{-r}, se mueve de tal modo que no salga del círculo trazado al rededor del punto 0 con un radio igual á 1. Los ocho puntos j^r dividen la circunferencia de este círculo en ocho octantes iguales, sobre los cuales se distribuyen los $\varphi(P)$ puntos ϑ^s que se reparten á su vez en las dos clases, ϑ^a y ϑ^b.

Ahora bien, de la definicion de $F(x)$ se desprenden algunas consecuencias interesantes. Desde luego, si designamos por x el valor com-

plejo conjugado de x, tenemos que dicha funcion, $F(x)$, es conjugada de esta otra

$$\Pi(x'-0^{-s})^{\left(\frac{s}{P}\right)} = F(x')^{\left(\frac{-1}{P}\right)};$$

y, por consecuencia, que $\dot{\psi}(r)$ y

$$\left(\frac{-1}{P}\right)\int_0^{j^r} d\log F(x') = \left(\frac{-1}{P}\right)\dot{\psi}(-r)$$

son asimismo conjugadas. Haciendo para abreviar

$$\begin{aligned} R(r) &= \dot{\psi}(-r) + \left(\frac{-1}{P}\right)\dot{\psi}(r) \\ J(r) &= \dot{\psi}(-r) - \left(\frac{-1}{P}\right)\dot{\psi}(r) \end{aligned} \qquad (4)$$

será, de consiguiente, R real, y J puramente imaginaria, ó cero; y no será difícil averiguar que la suma N se reduce á expresiones de la forma R, ó de la forma J, segun que la determinante D sea positiva ó negativa.

De la definicion de $F(x)$ se desprende tambien la relacion

$$F(x)F(-x) = F(x^2)^{\left(\frac{2}{P}\right)} \qquad (5)$$

y, como si x va desde 0 hasta j^{-r}, retrocede $-x^2$ desde 0 hasta $j^{-(r+4)}$, y x^2 desde 0 hasta j^{-2r}, resulta:

$$\dot{\psi}(r) + \dot{\psi}(r+4) = \left(\frac{2}{P}\right)\dot{\psi}(2r): \qquad (6)$$

poseyendo igual propiedad las expresiones R y J.

Por último, la funcion $F(x)$ comprende tambien esta otra:

$$F\left(\frac{1}{x}\right) = \prod^{\Sigma\left(\frac{s}{P}\right)^s} F(x)^{\left(\frac{-1}{P}\right)} \qquad (7)$$

de la cual, teniendo presente que cuando x, dentro del círculo, va desde 0 hasta j^{P}, su valor recíproco, y, fuera del círculo, retrocede desde ∞ hasta j^{P}, se deduce que:

$$\int_{\infty}^{j^P} d \log F(y) = \left(\frac{-1}{P}\right) \psi(r);$$

y, en consecuencia:

$$J(r) = \int_{0}^{\infty} d \log F(z_r),$$

cuando z_r marcha dentro del círculo desde 0 hasta j^{P}, y fuera del mismo desde j^{P} hasta ∞. Esto prueba que la diferencia $J(r)-J(r+1)$ es una integral definida, en la cual gira la variable en sentido positivo al rededor de los puntos 0^s que se hallan sobre el octante determinado por los j^{P} y j^{r+1}; y, por lo tanto:

$$J(r) - J(r+1) = 2\pi i \sum_{r}^{r+1} \left(\frac{s}{P}\right): \quad (*)$$

pudiendo recibir s todos los valores que satisfagan á la condicion

$$\frac{r}{8} < \frac{s}{P} < \frac{r+1}{8}.$$

Y de aquí resulta:

(*) Véase la nota final, pág. 600.

$$J(r) - J(r+4) = 2\pi i \sum_{r}^{r+4} \left(\frac{s}{P}\right);$$

y tambien, cuando r es *positivo:*

$$J(r) - J(2r) = 2\pi i \sum_{r}^{2r} \left(\frac{s}{P}\right).$$

Si introducimos los valores de $J(r+4)$ y $J(2r)$, deducidos de las dos últimas ecuaciones, en la siguiente que se desprende de la (6),

$$J(r) + J(r+4) = \left(\frac{2}{P}\right) J(2r),$$

se obtiene:

$$\left\{2 - \left(\frac{2}{P}\right)\right\} J(r) = 2\pi i \left\{\sum_{r}^{r+4} \left(\frac{s}{P}\right) - \left(\frac{2}{P}\right) \sum_{r}^{2r} \left(\frac{s}{P}\right)\right\};$$

y, teniendo presente que

$$\sum_{1}^{1+r} \left(\frac{s}{P}\right) = \left(\frac{-1}{P}\right) \sum_{1-r}^{1} \left(\frac{s}{P}\right),$$

estas otras:

$$\left\{2 - \left(\frac{2}{P}\right)\right\} J(0) = 2\pi i \sum_{0}^{1} \left(\frac{s}{P}\right)$$

$$\left\{2 - \left(\frac{2}{P}\right)\right\} J(2) = 2\pi i \left\{1 + \left(\frac{-1}{P}\right) - \left(\frac{2}{P}\right)\right\} \sum_{2}^{1} \left(\frac{s}{P}\right)$$

$$J(1) + \left(\frac{-1}{P}\right) J(3) = 2\pi i \left\{\sum_{1}^{1} \left(\frac{s}{P}\right) + \left(\frac{-1}{P}\right) \sum_{3}^{1} \left(\frac{s}{P}\right)\right\}.$$

Como, por último, segun las ecuaciones (6) y (4), tenemos tambien:

$$\psi(0) - \psi(4) = \left\{2 - \left(\frac{2}{P}\right)\right\} \psi(0)$$

$$\left\{1 - \left(\frac{-1}{P}\right)\right\} \psi(0) = J(0)$$

$$\psi(6) - \left(\frac{-1}{P}\right) \psi(2) = J(2)$$

$$\left\{\psi(7) - \psi(3)\right\} + \left(\frac{-1}{P}\right)\left\{\psi(5) - \psi(3)\right\} = J(1) + \left(\frac{-1}{P}\right) J(3);$$

se hallan, para la determinante *negativa* D, y, por consecuencia $P \equiv 3 \pmod 4$ en los casos primero y tercero, y $\equiv 1 \pmod 4$ en el segundo y cuarto, los valores de la série infinita N, que á continuacion se expresan:

I. $$N = \frac{\pi}{2\sqrt{P}} \sum_{0}^{4} \left(\frac{s}{P}\right)$$

II. $$N = \frac{\pi}{\sqrt{P}} \sum_{0}^{2} \left(\frac{s}{P}\right)$$

III. $$N = \frac{\pi}{\sqrt{2P}} \sum_{1}^{3} \left(\frac{s}{P}\right)$$

IV. $$N = \frac{\pi}{\sqrt{2P}} \left\{\sum_{0}^{1} \left(\frac{s}{P}\right) - \sum_{3}^{4} \left(\frac{s}{P}\right)\right\};$$

habiendo atendido á que, en el segundo y cuarto caso,

$$\sum_{0}^{1}\left(\frac{s}{P}\right)=0.$$

Para las determinantes *positivas* se obtienen asimismo notables simplificaciones en los valores de la série N.

De la expresion real (4)

$$R(r)=\int_{0}^{1}\sum\left(\frac{s}{P}\right)\left\{\frac{dx}{x-j^{r}\theta^{s}}+\frac{dx}{x-j^{r}\theta^{-s}}\right\}$$

$$=\sum\left(\frac{s}{P}\right)\log\left\{(j^{r}-\theta^{s})(j^{-r}-\theta^{-s})\right\}$$

$$=\log.\left\{F(j^{r})\,F(j^{-r})^{\left(\frac{-1}{P}\right)}\right\},$$

mediante la (7), se desprende esta otra:

$$R(r)=\log\left\{c\,F^{2}(j^{r})\right\}:$$

en la cual

$$c=\theta^{\Sigma b-\Sigma a}=\frac{-1+i\sqrt{3}}{2},\quad \text{ó}\quad =1,$$

segun $P=3$, ó diferente de 3. Por otra parte, segun las ecuaciones (4) y (6), tenemos:

$$\psi(0)-\psi(4)=\left\{2-\left(\frac{2}{P}\right)\right\}\psi(0)$$

$$\left\{1+\left(\frac{-1}{P}\right)\right\}\psi(0)=R(0)$$

$$\psi(6) + \left(\frac{-1}{P}\right)\psi(2) = R(2)$$

$$\psi(7) + \left(\frac{-1}{P}\right)\psi(1) = R(1)$$

$$\psi(5) + \left(\frac{-1}{P}\right)\psi(3) = R(3).$$

Luego, por ser, en el primero y tercer caso, $P \equiv 1 \pmod 4$, y en el segundo y cuarto $P \equiv 3 \pmod 4$, serán:

I. $$N \cdot 2\sqrt{P} = -\left\{1 - \left(\frac{2}{P}\right)\frac{1}{2}\right\} \log\{F^2(1)\}$$

II. $$N \cdot 2\sqrt{P} = -\log\{c\,F^2(i)\}$$

III. $$N \cdot 2\sqrt{2P} = \log \frac{F^2(j^3)}{F^2(j)}$$

IV. $$N \cdot 2\sqrt{2P} = -\log\{c^2 F^2(j) F^2(j^3)\}$$

178.—*Fórmulas finales para determinar el número de clases que buscamos.*

—

Determinado el valor de la série infinita N, para todos los casos en que la determinante D no sea divisible por ningun cuadrado, excepto la unidad, pasemos, por último, á expresar en forma concreta el número h de clases de formas primitivas, de primera especie, relativas á dicha determinante.

a) Para las determinantes *negativas*, obtuvimos (171) la ecuacion

$$h = \frac{2\sqrt{-D}}{\pi} . N$$

exceptuando la determinante -1, para la cual se duplica el segundo miembro.

De esta ecuacion se desprenden los cuatro resultados siguientes:

I. $D = -P \equiv 1 \pmod 4$; $\quad h = \sum_{0}^{4} \left(\frac{s}{P}\right)$

II. $D = -P \equiv 3 \pmod 4$; $\quad h = 2 \sum_{0}^{2} \left(\frac{s}{P}\right)$

III. $D = -2P \equiv 2 \pmod 8$; $\quad h = 2 \sum_{1}^{3} \left(\frac{s}{P}\right)$

IV. $D = -2P \equiv 6 \pmod 8$; $\quad h = 2 \left\{ \sum_{0}^{1} \left(\frac{s}{P}\right) - \sum_{3}^{1} \left(\frac{s}{P}\right) \right\}$

donde siempre se refieren los límites de la sumacion al valor $8s : P$; y exceptuando en el II y IV respectivamente los casos referentes á $D = -1$, $D = -2$ para los que es $h = 1$.

b) Para las determinantes *positivas* hallamos (173) la expresion

$$h \log (T + U\sqrt{D}) = N . 2\sqrt{D},$$

en la cual T, U representan los mínimos enteros, positivos, que satisfacen á la ecuacion

$$T^2 - D\,U^2 = 1,$$

y pueden hallarse siempre por el método explicado (158).

El valor de $N \cdot 2\sqrt{D}$ queda ya en el final del último párrafo determinado; pero en lugar de las fórmulas allí establecidas pueden tambien emplearse las siguientes, deducidas de la ecuacion (2) que figura en el mismo:

I. $D = P \equiv 1 \pmod 4$

$$h \log (T + U\sqrt{P}) = -\left\{4 - 2\left(\frac{2}{P}\right)\right\} \sum_{0}^{1} \left(\frac{n}{P}\right) \log \operatorname{sen} \frac{n\pi}{P}$$

II. $D = P \equiv 3 \pmod 4$

$$h \log (T + U\sqrt{P}) = -\sum_{0}^{4} \left(\frac{-1}{n}\right)\left(\frac{n}{P}\right) \log \operatorname{sen} \frac{n\pi}{4P}$$

III. $D = 2P \equiv 2 \pmod 8$

$$h \log (T + U\sqrt{2P}) = -\sum_{0}^{8} \left(\frac{2}{n}\right)\left(\frac{n}{P}\right) \log \operatorname{sen} \frac{n\pi}{8P}$$

IV. $D = 2P \equiv 6 \pmod 8$

$$h \log (T + U\sqrt{2P}) = -\sum_{0}^{8} \left(\frac{-2}{n}\right)\left(\frac{n}{P}\right) \log \operatorname{sen} \frac{n\pi}{8P}$$

donde n puede recorrer todos los números primos con $2P$, para los cuales $n : P$ caiga entre los límites de sumacion establecidos.

Las tres últimas fórmulas se compendian en la fórmula comun

$$h \log (T + U\sqrt{D}) = -\sum \left(\frac{D}{n}\right) \log \operatorname{sen} \frac{n\pi}{4D},$$

en la cual n representa todos los números primos con $4D$ y menores que este último.

NOTA.

Para àquellos de nuestros lectores que no conozcan al pormenor la teoría de las cantidades, llamadas por Gauss *complejas*, no dejarán de ser útiles las consideraciones siguientes:

Designemos por x, é y, y por $r\cos\varphi$, y $r\,\mathrm{sen}\,\varphi$, las coordenadas rectilíneas, y polares, de un punto, en un plano, referido á un sistema de ejes rectangulares situado en el mismo: la cantidad compleja

$$z = x + iy, \quad \text{ó} \quad z = r(\cos\varphi + i\,\mathrm{sen}\,\varphi),$$

estará representada por un punto en dicho plano, ó por una recta cuya longitud sea r y φ el ángulo que forme con el eje *principal*. La cantidad r se llama *módulo;* y la expresion $\cos\varphi + i\,\mathrm{sen}\,\varphi$ *coeficiente de direccion*.

Siendo las coordenadas x é y independientes una de otra, el punto z recorrerá un camino ó trayecto enteramente arbitrario; y sólo podrá exijirse, para que la variacion de z sea *contínua*, que tal trayecto lo forme una línea cualquiera, pero sin *rotura*.

Esto sentado, si hallamos la diferencial de una funcion

$$f(z) = w = u + iv$$

tambien de la misma forma que la cantidad compleja $z = x + iy$, y en la cual u y v significan funciones reales de x y de y, encontraremos que la condicion necesaria y suficiente para que la funcion w lo sea realmente de la cantidad compleja $z = x + iy$, se contiene en la ecuacion diferencial

$$\frac{dw}{dy} = i\frac{dw}{dx}.$$

Con estos antecedentes podemos ya fijar el concepto de integral definida respecto de las variables complejas, sin entretenernos en demostraciones, para explicar más clara y minuciosamente la que figura en el texto. En su fondo no difiere el concepto de integral definida, ya se refiera ésta á variables complejas, ya á variables reales; pero existe, sin embargo, entre unas y otras una diferencia notable, que

se deriva de la misma naturaleza de aquellas cantidades, á saber: que para marchar de un límite á otro en la integral de variable compleja pueden seguirse, no uno determinado, sino infinitos caminos, de los cuales depende el valor de la integral definida correspondiente. Por esta razon la ley

$$\int_{z_0}^{z} f(z)\,dz = F(z) - F(z_0)$$

que es exacta para las variables reales, siempre que $f(z)$ exprese la derivada de $F(z)$, no lo es, en general, para las variables complejas; puesto que, segun hemos indicado, el valor de la integral para estas variables no depende solamente de sus límites, superior é inferior, ó extremos; sino tambien de los valores que adquieran sus elementos diferenciales para valores comprendidos entre aquellos límites.

Imaginemos ahora una porcion de plano, determinada de cualquier modo; y admitamos que P y Q son dos funciones reales de x é y, que no dejen de ser finitas y contínuas para todos los valores que puedan recibir estas variables dentro de la porcion superficial marcada. La integral que comprende toda esta porcion,

$$\int\int \left(\frac{dQ}{dx} - \frac{dP}{dy}\right) dx\,dy,$$

es igual á la integral lineal,

$$\int (P\,dx + Q\,dy),$$

que abraza el contorno entero de la misma.

Si la expresion

$$P\,dx + Q\,dy$$

fuese una diferencial completa, la integral

$$\int (P\,dx + Q\,dy)$$

referida al contorno entero de una porcion de plano, dentro del cual permanecierau P y Q finitas y contínuas, sería igual á *cero*, como se demuestra en los Cálculos. Así, pues, siendo la condicion, para que $Pdx+Qdy$ sea una diferencial completa,

$$\frac{dP}{dy} = -\frac{dQ}{dx}.$$

y esta otra, ya conocida,

$$\frac{dw}{dy} = i\,\frac{dw}{dx} = \frac{d\,(i\,w)}{dx},$$

para que w sea funcion de z, la diferencial

$$w\,dx + i\,w\,dy = w\,(dx + i\,dy) = w\,dz = f(z)\,dz$$

será completa, y por consecuencia:

$$\int f(z)\,dz = 0:$$

con tal que $f(z)$ permanezca finita y contínua dentro de la porcion de superficie á cuyo contorno se extiende la integral última. No variará ésta de valor, aunque se refiera á dos contornos diferentes, pero que comiencen y acaben en los mismos puntos, si la funcion $f(z)$, dentro de la porcion de superficie enteramente definida por aquéllos, satisface á la condicion ya expresada. Sólo cuando no suceda esto, es decir, sólo cuando deje de ser finita $f(z)$ para alguno ó vários puntos de la superficie encerrada por el contorno á que la integral en cuestion se refiere, no podremos afirmar que tal integral sea cero; pero entónces, cualquiera que sea su valor, no se alterará porque añadamos ó quitemos á la superficie, dentro de la cual hay puntos para los cuales $f(z)$ no es finita ni contínua, porciones de superficies en las que se verifique la condicion antes impuesta á $f(z)$.

En general, siempre que existan puntos de discontinuidad en una superficie se reemplazan por curvas cerradas muy pequeñas que los rodéen, y se consideran estas curvas como pertenecientes al contorno de la superficie propuesta.

En conformidad con la doctrina anterior hemos impuesto á la variable z la condicion de mantenerse dentro del círculo desde 0 hasta j^r, y fuera de él, desde j^r hasta ∞; pues los únicos valores que, en el caso del texto, hacen infinita la funcion diferencial, son los θ^s, distintos todos de los j^r, y situados sobre el mismo círculo unos y otros. Designemos por a uno de los puntos θ^s; teniendo en cuenta que el elemento diferencial es

$$\left(\frac{s}{P}\right)\frac{dx}{x - j^r\,\theta^s} = \left(\frac{s}{P}\right)\frac{dz}{z - 0^s},$$

puesto que $z = xj^{-r}$ ó $x = zj^r$; la integral correspondiente deberá extenderse, ó tomarse á lo largo de una línea cerrada que rodée al punto a, y que no contenga ella á su vez puntos de aquella especie; y entre todas estas líneas, la más sencilla es una circunferencia cuyo centro sea a, y su radio r, infinitamente pequeño. Podemos escribir en consecuencia:

$$z - a = r(\cos\varphi + i \operatorname{sen}\varphi),$$

de donde, considerando que, cuando z recorre el pequeño círculo, en el sentido de aumentar los ángulos, r permanece constante, y φ varia desde 0 hasta 2π, resulta:

$$dz = r(-\operatorname{sen}\varphi + i\cos\varphi)\,d\varphi = i\,r(\cos\varphi + i\operatorname{sen}\varphi)\,d\varphi;$$

y por tanto:

$$\frac{dz}{z-a} = i\,d\varphi.$$

Con esto la integral del texto adquiere el valor

$$\int_0^{2\pi} \left(\frac{s}{P}\right) \frac{dz}{z-a} = 2\pi i \left(\frac{s}{P}\right)$$

para el punto a; y como otro tanto puede decirse de los 0^s puntos, comprendidos en el octante determinado por los j^r y j^{r+1}, resulta finalmente la expresion anotada (pág. 593).

APÉNDICES.

I.

De las fracciones contínuas.

1.—*Algoritmo de Euler.*

Este algoritmo (*), de grande importancia en las fracciones contínuas, y de influencia tambien, como hemos visto ya, en otras investigaciones, se funda en los sencillos principios que á continuacion se exponen.

Sean

$$a,\ b, \tag{1}$$

dos cantidades indeterminadas cualesquiera, y

$$\gamma, \delta, \varepsilon, \ldots\ldots \lambda, \mu, \nu \tag{2}$$

una série de cantidades, tambien indeterminadas, hasta en su número ó conjunto; y con las unas y las otras formemos otra série, $c, d, e, \ldots\ldots l, m, n,$ del modo siguiente:

$$\begin{aligned} c &= \gamma b + a \\ d &= \delta c + b \\ e &= \varepsilon d + c \\ &\ldots\ldots\ldots \\ &\ldots\ldots\ldots \\ n &= \nu m + l \end{aligned} \tag{3}$$

(*) Euleri, *Comm. arithm.*, t. II. *De usu novi algorithmi*..... etc. Gauss. D. A. §. 27.

Introduciendo ahora en el valor de d el que corresponde á c, tendremos:

$$d = \delta a + (\gamma \delta + 1) b,$$

que consta de dos términos: uno que contiene al factor a, y el otro al b. Sustituyendo, en el valor de e, la d por su valor últimamente hallado, y la c por el establecido, resultará una expresion para el valor de e, de la misma forma hallada para el de d; y, prosiguiendo así hasta obtener el de n, por él veremos que la ley, reconocida en los dos casos mencionados, es general: circunstancia cumplida necesariamente en cuanto demos por sentado que l y m tienen ya la forma de los dos primeros términos. En consecuencia, podemos escribir la igualdad

$$n = G a + H b:$$

en la cual G y H serán independientes de a y b; sin que haya inconveniente tampoco en expresar el coeficiente H, que depende exclusivamente de los elementos de la série (2), por el símbolo

$$[\gamma, \delta, \varepsilon, \ldots\ldots \lambda, \mu, \nu] \qquad (4)$$

que vamos á utilizar en la demostracion de algunos teoremas interesantes.

Concíbese desde luego que si, en vez de las séries (1) y (2), tomásemos como puntos de partida estas otras,

$$b, \quad c, \qquad (1')$$

y

$$\delta, \varepsilon, \ldots\ldots \lambda, \mu, \nu \qquad (2')$$

podrian obtenerse, segun el mismo procedimiento de antes, los términos $d, e, \ldots\ldots l, m, n$; y los dos valores de n, deducidos, primero de los elementos (1) y (2), y despues de los (1') y (2'), serian respectivamente:

$$n = G a + [\gamma, \delta, \varepsilon, \ldots\ldots \lambda, \mu, \nu] b$$

$$n = G' b + [\delta, \varepsilon, \ldots\ldots \lambda, \mu, \nu] c.$$

Si ponemos en esta última expresion por c su valor $\gamma b + a$, se obtiene esta otra:

$$n = [\delta, \varepsilon, \ldots\ldots \lambda, \mu, \nu]\, a + (\gamma\, [\delta, \varepsilon, \ldots\ldots \lambda, \mu, \nu] + G')\, b$$

y, comparando los coeficientes de a en las dos expresiones de n, resulta:

$$G' = [\delta, \varepsilon, \ldots\ldots \lambda, \mu, \nu]:$$

esto es, G representado por un símbolo semejante al de H, mediante el cual la primera de aquellas se convierte en

$$n = [\delta, \varepsilon, \ldots\ldots \lambda, \mu, \nu]\, a + [\gamma, \delta, \varepsilon, \ldots\ldots \lambda, \mu, \nu]\, b;$$

y, como por iguales motivos debe ser tambien

$$G' = [\varepsilon, \ldots\ldots \lambda, \mu, \nu],$$

de la comparacion de los coeficientes de b, en los dos últimos valores de n, resulta finalmente:

$$[\gamma, \delta, \varepsilon, \ldots\ldots \lambda, \mu, \nu] = \gamma\, [\delta, \varepsilon, \ldots\ldots \lambda, \mu, \nu] + [\varepsilon, \ldots\ldots \lambda, \mu, \nu] \qquad (5)$$

que expresa la ley de formacion hácia la izquierda de los símbolos (4).

Una ley semejante, para la formacion hácia la derecha de estas expresiones simbólicas, se obtiene por la consideracion sencilla de que, en el supuesto $a = 0$, $b = 1$, las cantidades l, m, n se convierten respectivamente en los símbolos:

$$[\gamma, \ldots\ldots \lambda], \quad [\gamma \ldots\ldots \lambda, \mu], \quad [\gamma, \ldots\ldots \lambda, \mu, \nu]:$$

entre los cuales existe la relacion

$$[\gamma, \ldots\ldots \lambda, \mu, \nu] = [\gamma, \ldots\ldots \lambda, \mu]\, \nu + [\gamma, \ldots\ldots \lambda]. \qquad (6)$$

De las dos leyes (5) y (6) se desprende la siguiente:

$$[\nu, \mu, \ldots\ldots \delta, \gamma] = [\gamma, \delta, \ldots\ldots \mu, \nu]. \qquad (7)$$

Para demostrarla, admitamos que se verifica para expresiones con menor número de elementos: de modo que, por ejemplo, sean:

$$[\delta, \varepsilon, \ldots\ldots \nu] = [\nu, \ldots\ldots \varepsilon, \delta], \quad [\varepsilon, \ldots\ldots \nu] = [\nu, \ldots\ldots \varepsilon]:$$

de la (5) entónces se deduce:

$$[\gamma, \delta, \varepsilon, \ldots\ldots \nu] = [\nu, \ldots\ldots \varepsilon, \delta]\,\gamma + [\nu, \ldots\ldots \varepsilon]$$

y, combinando ésta con la (6), se prueba inmediatamente la exactitud de la (7). Mas la ley en cuestion se verifica en realidad para los primeros casos; pues, cuando el símbolo contiene un solo elemento, γ, es evidente; y, cuando contiene dos, es tambien:

$$[\gamma, \delta] = \gamma\,\delta + 1 = [\delta, \gamma]:$$

luego será cierta para cualquier número de elementos $\gamma, \delta, \ldots\ldots \mu, \nu$.

Las ecuaciones (3) que expresan la ley de formacion de los términos $c, d, e, \ldots\ldots l, m, n,$ pueden escribirse además de este otro modo:

$$-c = (-\gamma)\,b + (-a)$$
$$+d = (-\delta)(-c) + b$$
$$-e = (-\varepsilon)\,d + (-c)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\pm n = (-\nu)(\mp m) + (\pm l);$$

debiéndose tomar en la última el signo superior, ó el inferior, segun que el número de los elementos $\gamma, \delta, \varepsilon, \ldots\ldots \lambda, \mu, \nu$ sea par, ó impar. De estas nuevas ecuaciones se colije que la série $-c, +d, -e, \ldots\ldots \pm n$

puede formarse, por el mismo procedimiento antes empleado, partiendo de los primeros términos,

$$-a, \quad b, \tag{1''}$$

y de la série

$$-\gamma, -\delta, -\varepsilon, \ldots\ldots -\lambda, -\mu, -\nu. \tag{2''}$$

Entónces será tambien:

$$\pm n = [-\delta, -\varepsilon, \ldots\ldots -\nu](-a) + [-\gamma, -\delta, -\varepsilon, \ldots\ldots -\nu]\, b$$

y, por consecuencia:

$$[-\gamma, -\delta, \ldots\ldots -\nu] = \pm [\gamma, \delta, \ldots\ldots \nu] \tag{8}$$

en cuyo segundo miembro deberá tomarse el signo superior, ó el inferior, segun que el número de los elementos $\gamma, \delta, \ldots\ldots \nu$, sea par, ó impar.

Por último, las ecuaciones (3) pueden escribirse además, en sentido inverso, como sigue:

$$l = (-\nu)\, m + n$$

$$k = (-\mu)\, l + m$$

$$\ldots\ldots\ldots\ldots$$

$$\ldots\ldots\ldots\ldots$$

$$b = (-\delta)\, c + d$$

$$a = (-\gamma)\, b + c$$

En consecuencia será:

$$\pm a = [-\mu, \ldots\ldots -\gamma]\, n + [-\nu, -\mu, \ldots\ldots -\gamma]\, m,$$

ó, aplicando la ley (8):

$$\pm a = -[\mu, \ldots . \gamma]\, n + [\nu, \mu, \ldots . \gamma]\, m;$$

ó, si se tiene en cuenta la (7):

$$\pm a = -[\gamma, \delta \ldots . \mu]\, n + [\gamma, \delta, \ldots . \mu, \nu]\, m.$$

Si suponemos ahora $a = 1$, $b = 0$, los términos m, n quedarán representados por los símbolos,

$$[\delta, \ldots . \mu], \quad [\delta, \ldots . \mu, \nu],$$

respectivamente: de todo lo cual resulta:

$$\pm 1 = [\delta, \ldots . \mu]\,[\gamma, \delta, \ldots . \mu, \nu] - [\delta, \ldots . \mu, \nu]\,[\gamma, \delta, \ldots . \mu]: \qquad (9)$$

debiéndose tomar el signo superior, ó el inferior, segun que el número de los elementos $\gamma, \delta \ldots . \mu, \nu$ sea par, ó impar.

Aplicacion.—Escribamos las ecuaciones establecidas (69) para resolver la ecuacion de primer grado $ax - by = 1$ del modo siguiente:

$$c = (-\gamma)\, b + a$$

$$d = (-\gamma)\, c + b$$

. . . . . .

. . . . . .

$$1 = (-\nu)\, m + l$$

é inmediatamente se obtiene:

$$1 = [-\delta, -\varepsilon, \ldots . -\mu, -\nu]\, a + [-\gamma, -\delta, -\varepsilon, \ldots . -\mu, -\nu]\, b$$

ó, conforme á la ley (8):

$$1 = \mp [\delta, \varepsilon, \ldots . \mu, \nu]\, a \pm [\gamma, \delta, \varepsilon, \ldots . \mu, \nu]\, b,$$

y, por consecuencia, la solucion:

$$x = \mp [\delta, \varepsilon, \ldots\ldots \mu, \nu] \quad y = \mp [\gamma, \delta, \varepsilon, \ldots\ldots \mu, \nu];$$

y una raiz x, tambien, de la congruencia

$$a x \equiv 1 \pmod{b}.$$

Por via de ejemplo resolveremos la misma congruencia

$$37 x \equiv 1 \pmod{100}$$

del artículo (69). Del cálculo allí efectuado se deducen:

$$\gamma = 0, \quad \delta = 2, \quad \varepsilon = 1, \quad \lambda = 2, \quad \mu = 2, \quad \nu = 1;$$

y, como el número de estos elementos es par, será

$$x \equiv - [2, 1, 2, 2, 1] \pmod{100}.$$

Efectuado el cálculo del símbolo $\equiv x$, de derecha á izquierda, tendremos:

$$[1] = 1; \ [2, 1] = 3; \ [2, 2, 1] = 7; \ [1, 2, 2, 1] = 10; \ [2, 1, 2, 2, 1] = 27:$$

y, de consiguiente,

$$x \equiv - 27 \equiv 73 \pmod{100}.$$

Este modo de calcular el valor de x, empezando por la derecha y hácia la izquierda, es ventajoso para obtener el de y, que se halla entónces sencillamente, segun la ley (5), en cuanto conozcamos los valores de los símbolos

$$[\varepsilon, \ldots\ldots \mu, \nu] \qquad \text{y} \qquad [\delta, \varepsilon, \ldots\ldots \mu, \nu].$$

Siempre que sea $\gamma = 0$, como acontece en el ejemplo actual, el valor de y, conforme á la citada ley (5), se reduce á este otro:

$$y = \mp [\varepsilon, \ldots\ldots \mu, \nu]:$$

luego finalmente:

$$y = -[0, 2, 1, 2, 2, 1] = -[1, 2, 2, 1] = 10.$$

2.—*Fracciones continuas.*

a) Sea x una cantidad positiva, racional ó irracional, y establezcamos la série de igualdades:

$$x = \gamma + \frac{1}{x_1} \quad x_1 = \delta + \frac{1}{x_2}, \ldots\ldots x_{n-1} = \nu + \frac{1}{x_n} \ldots\ldots \qquad (1)$$

en las que $\gamma, \delta, \ldots\ldots \nu$, representan los máximos enteros, contenidos en x_1, $x_2 \ldots\ldots x_{n-1}$ respectivamente: todos ellos iguales, por lo ménos, á 1, excepto el primero γ, que tambien puede ser 0.

Si la cantidad x fuese racional, alguno de los números $x, x_1, x_2, \ldots\ldots$ sería entero, y en él terminaria la série (1); pues el siguiente, conforme á la ley de su formacion, llegaria á ser infinito. Para demostrar que la série (1) es finita, siempre que x sea racional, hagamos esta cantidad igual al quebrado irreducible $a : b$. De la série de igualdades que se derivan del algoritmo ya demostrado (40) para hallar el máximo comun divisor m de los números a y b, resultan las siguientes:

$$x = \frac{a}{b} = \gamma + \frac{c}{b}; \quad x_1 = \frac{b}{c} = \delta + \frac{d}{c}; \ldots\ldots x_{n-1} = \frac{l}{m} = \nu + \frac{1}{m};$$

$$x_n = \frac{m}{1} = m:$$

donde se ve patentemente que el cociente x_n es entero; y, por conse-

cuencia, 0, el resíduo de su division correspondiente, é infinito ya el cociente sucesivo.

Si x fuera irracional, ninguno de los términos $x, x_1, x_2 \ldots\ldots$ sería entero, ni áun racional; y aquella série podria entónces prolongarse indefinidamente; porque, si alguno de dichos términos fuera racional, es claro que lo habrian de ser tambien todos los precedentes.

Esto sentado, eliminando las cantidades $x_1, x_2 \ldots\ldots x_{n-1}$ entre las n igualdades primeras de la série (1), la expresion del valor de x será la siguiente:

$$x = \gamma + \cfrac{1}{\delta + \cfrac{1}{\varepsilon + \cfrac{1}{\ddots + \cfrac{1}{\nu + \cfrac{1}{x_n}}}}} \qquad (2)$$

Esta expresion será finita, esto es, podrá en ella suprimirse el término $\frac{1}{x_n}$, en el supuesto de que x sea racional; pues ya hemos demostrado que entónces existe siempre un valor de n para el cual es $x_n = \infty$. Esto no podrá efectuarse en el caso de ser x irracional; mas luego probaremos que, áun en esta hipótesis, el segundo miembro de la fórmula (2), despues de suprimido el quebrado $\frac{1}{x_n}$, converge hácia el valor de x, si n crece indefinidamente.

Las expresiones de la forma

$$\gamma + \cfrac{1}{\delta + \cfrac{1}{\varepsilon + \cfrac{1}{\ddots + \cfrac{1}{\nu + \cfrac{1}{\ddots}}}}} \qquad (3)$$

se llaman *fracciones contínuas;* los términos de la série (1) *cocientes completos;* y los *enteros*, $\gamma, \delta, \ldots \nu$, contenidos en aquellos cocientes completos, se denominan *cocientes incompletos.* Las fracciones contínuas, como la escrita (3), cuyos numeradores son todos iguales á la unidad, se llaman *ordinarias;* y llevan además el nombre de *regulares,* si todos sus elementos $\gamma, \delta, \ldots \nu, \ldots$ excepto el primero que puede ser 0, son *positivos.*

Las fracciones contínuas se representan abreviadamente por medio de un paréntesis que comprende todos sus elementos. Así, por ejemplo, la fraccion contínua ordinaria, regular (3), en el supuesto de ser finita, ó terminar en el cociente ν, será igual á

$$(\gamma, \delta, \varepsilon, \ldots \mu, \nu).$$

Y, por consecuencia de este simbolismo:

$$(\gamma, \delta, \varepsilon, \ldots \lambda, \mu, \nu) = \gamma + \frac{1}{(\delta, \varepsilon, \ldots \lambda, \mu, \nu)} = \left(\gamma, \delta, \varepsilon, \ldots \lambda, \mu + \frac{1}{\nu}\right).$$

Veamos ahora si este nuevo símbolo se comprende en el empleado para el *algoritmo de Euler*, ó bien, si se verifica en general:

$$(\gamma, \delta, \varepsilon \ldots \mu, \nu) = \frac{[\gamma, \delta, \varepsilon \ldots \mu, \nu]}{[\delta, \varepsilon, \ldots \mu, \nu]}. \qquad (4)$$

Admitamos, pues, que así sucede para un número menor de elementos; y que sea, en consecuencia:

$$(\delta, \varepsilon, \ldots \mu, \nu) = \frac{[\delta, \varepsilon, \ldots \mu, \nu]}{[\varepsilon, \ldots \mu, \nu]}.$$

Poniendo el segundo miembro de esta igualdad por el primero en la precedente

$$(\gamma, \delta, \varepsilon, \ldots \mu, \nu) = \gamma + \frac{1}{(\delta, \varepsilon, \ldots \mu, \nu)}.$$

resulta esta otra:

$$(\gamma, \delta, \varepsilon, \ldots\ldots \mu, \nu) = \gamma + \frac{[\varepsilon, \ldots\ldots \mu, \nu]}{[\delta, \varepsilon, \ldots\ldots \mu, \nu]} = \frac{\gamma\,[\delta, \varepsilon, \ldots\ldots \mu, \nu] + [\varepsilon, \ldots\ldots \mu, \nu]}{[\delta, \varepsilon, \ldots\ldots \mu, \nu]}$$

de la cual, teniendo presente la ley (5) del artículo anterior, se desprende la (4).

Mas esta igualdad (4) se verifica evidentemente para un sólo elemento; y es cierta tambien para dos, porque

$$(\gamma, \delta) = \gamma + \frac{1}{\delta} = \frac{\gamma\,\delta + 1}{\delta} = \frac{[\gamma, \delta]}{[\delta]};$$

luego lo será, en general, para cualquier número de elementos.

b) Las fracciones parciales

$$(\gamma), \quad (\gamma, \delta), \quad (\gamma, \delta, \varepsilon), \quad (\gamma, \delta, \varepsilon, \zeta), \ldots\ldots \qquad (5)$$

se llaman *aproximadas* ó *convergentes;* pues se van sucesivamente acercando á la (4), que es igual á la cantidad x; y el número de elementos que contienen marca su órden, ó lugar en la série. El procedimiento para convertir en *contínua* la fraccion *ordinaria,* irreducible,

$$x = \frac{a}{b},$$

queda ya suficientemente explicado; el que habrá de emplearse para convertir, por el contrario, las contínuas (5) en ordinarias, se colige inmediatamente de la fórmula (4). Así efectivamente se hallan:

$$\frac{[\gamma]}{1}, \quad \frac{[\gamma, \delta]}{[\delta]}, \quad \frac{[\gamma, \delta, \varepsilon]}{[\delta, \varepsilon]}, \quad \frac{[\gamma, \delta, \varepsilon, \zeta]}{[\delta, \varepsilon, \zeta]}, \ldots\ldots \qquad (6)$$

ó bien, aplicando la ley (6) del artículo anterior para la formacion de estos símbolos:

$$\frac{\gamma}{1}, \frac{\gamma\delta+1}{\delta}, \frac{(\gamma\delta+1)\varepsilon+\gamma}{\delta\varepsilon+1}, \frac{((\gamma\delta+1)\varepsilon+\gamma)\zeta+(\gamma\delta+1)}{(\delta\varepsilon+1)\zeta+\delta}, \ldots\ldots \qquad (6')$$

Con esta explícita representacion de las aproximadas es fácil traducir la ley (6) del art. 1 al lenguaje vulgar del modo siguiente: *formadas como de ordinario las dos primeras, que corresponden á los dos primeros cocientes, cualquiera de las otras se formará multiplicando por el cociente respectivo los dos términos de la inmediata anterior, y sumando con cada uno de los productos los dos términos de la anterior en dos lugares respectivamente.*

Efectuando las multiplicaciones indicadas en los términos de las fracciones (6'), se obtienen estas otras:

$$\frac{\gamma}{1}, \frac{\gamma\delta+1}{\delta}, \frac{\varepsilon\delta\gamma+\varepsilon+\gamma}{\varepsilon\delta+1}, \frac{\zeta\varepsilon\delta\gamma+\zeta\varepsilon+\zeta\gamma+\delta\gamma+1}{\zeta\varepsilon\delta+\zeta+\delta}, \ldots\ldots;$$

donde se ve que los denominadores de cada una se deducen fácilmente de los numeradores de las inmediatas anteriores, sustituyendo los elementos que figuran en éstos por los inmediatos siguientes: esto es, γ por δ; δ por ε; etc.

De la ley para la formacion de las aproximadas se desprende asimismo, que los términos de cualquiera de ellas son mayores respectivamente que los de cada una de las precedentes; y además que son enteros, si lo son los elementos $\gamma, \delta \ldots\ldots \mu, \nu$.

c) En la ecuacion (9) del art. 1 se fundan algunas propiedades interesantes de las aproximadas. En ella figura la diferencia de los productos en cruz de los numeradores y denominadores de las dos aproximadas consecutivas,

$$\frac{[\gamma, \delta, \ldots\ldots \mu]}{[\delta, \ldots\ldots \mu]} \quad \text{y} \quad \frac{[\gamma, \delta, \ldots\ldots \mu, \nu]}{[\delta, \ldots\ldots \mu, \nu]};$$

y aquella diferencia, si designamos estas fracciones respectivamente por

$$\frac{P_{n-1}}{Q_{n-1}} \quad \text{y} \quad \frac{P_n}{Q_n}.$$

siendo n el número de los cocientes $\gamma, \delta, \ldots\ldots \mu, \nu$, que entran en la última, podrá escribirse de este modo más breve:

$$P_n\, Q_{n-1} - Q_n\, P_{n-1} = (-1)^n \qquad (7)$$

Importa advertir, antes de pasar adelante, que se halla á nuestro arbitrio hacer que el exponente n, ó el número de los elementos comprendidos en la última fraccion $P_n : Q_n$, sea par ó impar. En efecto, el último ν, de tales elementos, segun el procedimiento para desarrollar una fraccion ordinaria en contínua, no puede ser 1; porque, si lo fuera, se agregaria al anterior μ, convirtiéndose éste así en $\mu + 1$; y, debiendo ser ν por lo ménos igual á 2, no hay inconveniente en hacer $\nu = \nu - 1 + \frac{1}{1}$: con lo cual será

$$[\gamma, \delta, \ldots\ldots \mu, \nu] = [\gamma, \delta, \ldots\ldots (\nu - 1), 1].$$

La igualdad (7) prueba desde luego (69) que *los términos de las aproximadas son primos entre sí;* y, por consecuencia, que *tales fracciones son irreducibles.*

Y esta otra, derivada de aquélla,

$$\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^n}{Q_n\, Q_{n-1}}, \qquad (8)$$

manifiesta que *la diferencia entre dos aproximadas, consecutivas, es igual á un quebrado, cuyo numerador es la unidad, y cuyo denominador es el producto de los denominadores de aquéllas.*

Por el aspecto mismo de las aproximadas se colige, y reparando en ellas se prueba inmediatamente, que la primera es menor, la segunda mayor, y, en general, las de lugar par mayores, y las de lugar impar menores que la cantidad x: comprendida, por lo tanto, entre dos aproximadas consecutivas; y además, que á dicha cantidad x se van acercando sucesivamente las aproximadas, justificándose de este modo su nombre. Si, pues, la diferencia entre dos aproximadas, consecutivas, es

la escrita (8), la diferencia entre la cantidad x y una cualquiera de ellas será

$$< \frac{(-1)^n}{Q_n Q_{n-1}}.$$

Designemos ahora por $a:b$ una fraccion irreducible, comprendida entre dos aproximadas; es claro que las diferencias

$$\frac{a}{1} - \frac{P_{n-1}}{Q_{n-1}} \quad \text{y} \quad \frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}}$$

tendrán el mismo signo, siendo el valor absoluto de la primera menor que el de la segunda, ya conocido (8); por lo cual:

$$(-1)^n \left(\frac{a}{b} - \frac{P_{n-1}}{Q_{n-1}} \right) < \frac{1}{Q_n Q_{n-1}},$$

ó bien:

$$(-1)^n (a Q_{n-1} - b P_{n-1}) < \frac{b}{Q_n}.$$

Mas el primer miembro de esta desigualdad es un entero: luego necesariamente habrá de ser $b > Q_n$, y con mayor razon $> Q_{n-1}$. En lenguaje vulgar quiere decir lo demostrado que *entre dos aproximadas consecutivas no puede existir fraccion irreducible, cuyo denominador no sea mayor que los de aquellas.* De esta proposicion se deduce la consecuencia importante de que *no puede existir fraccion irreducible, con denominador menor que el de una aproximada, que se acerque más que ésta al valor de* x.

Y hé aquí por qué se da tambien justamente á las aproximadas el nombre de *reducidas.*

d) Siendo las reducidas de lugar par mayores, y las de lugar im-

par menores que la cantidad x, generativa de la fraccion contínua (3), y aproximándose todas ellas cada vez más y sucesivamente al valor de x, resulta que las reducidas de lugar impar formarán una série creciente, y las de lugar par, por el contrario, una série decreciente. En el caso de ser x racional, dichas séries son finitas; y no lo serán en el caso contrario, esto es, cuando x sea irracional. Respecto del primero, dijimos que la última reducida, la que comprendia todos los elementos $\gamma, \delta, \ldots\ldots \mu, \nu$, de la fraccion contínua, era igual á la cantidad racional x; en cuanto al segundo, haremos notar que la reducida $P_n : Q_n$ tiene por expresion la siguiente:

$$\frac{P_1}{Q_1} + \left(\frac{P_2}{Q_2} - \frac{P_1}{Q_1}\right) + \left(\frac{P_3}{Q_3} - \frac{P_2}{Q_2}\right) + \ldots\ldots + \left(\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}}\right),$$

y, por lo tanto, la cantidad x es el límite de la série (ecuacion 8)

$$\frac{\gamma}{1} + \frac{1}{Q_1 Q_2} - \frac{1}{Q_2 Q_3} + \ldots\ldots + \frac{(-1)^n}{Q_{n-1} Q_n} + \ldots\ldots,$$

que, por estar compuesta de términos, alternativamente positivos y negativos, y todos ellos decrecientes, se halla dentro de las condiciones de convergencia.

Mas el justificar de este modo el empleo de las fracciones contínuas, infinitas, en el cálculo, supone que los cocientes incompletos, ó denominadores parciales de las mismas, son enteros y positivos. Prescindiendo de pormenores (*) acerca de tales fracciones infinitas, despues de lo escrito en los artículos 155 y 156 del texto, y concretándonos á lo más indispensable, vamos á tratar ahora de las fracciones contínuas, cuyos elementos no sean todos enteros y positivos, esto es, de las que llamamos *irregulares*.

(*) Puede consultar el lector que lo necesite: los dos primeros Capítulos del *Serret*, Alg. sup., tomo I; el IX de la segunda parte del *Berkhan: Die Auflösung der Dioph. Gleichungen;* y el §-6 de la *Zahlen-Theorie* por *Schwarz*.

e) Sabido es que el valor de una fraccion *regular*, finita ó infinita, es siempre positivo; como tambien, recíprocamente, que toda cantidad *positiva*, racional ó irracional, puede desarrollarse siempre, y *de un solo modo*, en fraccion contínua. Mas el valor de una fraccion *irregular*, cuyos elementos, á contar desde uno cualquiera de ellos, no sean positivos, no puede saberse, por lo dicho antes, si será positivo ó negativo; é interesa mucho convertir en regular una fraccion de aquella especie para de este modo afirmarlo.

Dada la fraccion irregular, que se ha de trasformar,

$$(\alpha, \beta, \gamma, \ldots\ldots \mu, \nu, p, q, r, \ldots\ldots u, v, \ldots\ldots),$$

supongamos que sea ν el último elemento, no positivo, y que no sea además el primero de toda ella. El procedimiento de conversion consiste en apartar la irregularidad de su sitio extremo ν, y correrla un lugar, por lo ménos, hácia la izquierda; repitiendo esto mismo cuantas veces sea necesario. Por tal procedimiento se manifestará que *todos los elementos* $u, v, \ldots\ldots$, *á contar desde uno determinado* u, *situado á distancia finita, permanecen inalterables; y que la diferencia entre el número de los elementos variados ó sustituidos, y el número de los sustitutos, es par, ó impar, segun que el valor de la fraccion entera sea positivo, ó negativo.*

Consideremos, pues, y basta para nuestro objeto, la fraccion infinita

$$(\mu, \nu, p, q, r, s, \ldots\ldots u, v, \ldots\ldots)$$

que puede expresarse tambien bajo las formas finitas,

$$(\mu, \nu, p'), \quad (\mu, \nu, p, q'), \quad (\mu, \nu, p, q, r'),$$

si por abreviar establecemos las igualdades

$$(p, q, r, s, \ldots\ldots u, v, \ldots\ldots) = p', \quad (q, r, s \ldots\ldots u, v \ldots\ldots) = q',$$

$$(r, s, \ldots\ldots u, v, \ldots\ldots) = r'.$$

Al calificar al elemento ν de no positivo, en lugar de negativo resueltamente, ya indicamos que ν, sin ser positivo, podia ser *cero*, ó *negativo;* de modo que en esta cuestion debemos examinar dos casos.

1.° $\nu = 0$. En tal hipótesis será

$$(\mu, 0, p') = \mu + \frac{1}{0 + \frac{1}{p}} = \mu + p' = \mu + p + \frac{1}{q'},$$

y, por consecuencia:

$$(\mu, 0, p, q,') = (\mu + p, q').$$

Lo cual prueba que la irregularidad se ha corrido un lugar, por lo menos, á la izquierda de $\nu = 0$; y que en vez de los tres elementos variados, $\mu, 0, p$, figura uno solo, $\mu + p$.

2.° $\nu = -n$ que comprende dos particulares: $n > 1$ y $n = 1$.

Si $n > 1$, con auxilio de la igualdad evidente

$$(g, -h) = g - \frac{1}{h} = g - 1 + 1 - \frac{1}{h} = g - 1 + \frac{1}{1 + \frac{1}{h-1}} =$$

$$= (g - 1, 1, h - 1)$$

obtendremos las siguientes trasformaciones:

$$(\mu, -n, p') = \mu + \frac{1}{-n + \frac{1}{p'}} = \left(\mu, -\left(n - \frac{1}{p'}\right)\right) =$$

$$= (\mu - 1, 1, n - 1 - \frac{1}{p'}) = (\mu - 1, 1, n - 1, -p');$$

y de esta última expresion, aplicando de nuevo la misma igualdad:

$$(\mu,-n,p,q') = (\mu-1,1,n-2,1,p'-1) = (\mu-1,1,n-2,1,p-1,q).$$

Cotejando las dos fracciones extremas, inmediatas, se nota que, en lugar de los *tres* elementos $\mu, -n, p$, que figuran en la primera, aparecen los *cinco*, $\mu-1, 1, n-2, 1, p-1$, en la segunda; de los cuales el primero, á lo sumo, puede ser negativo. Si, por otra parte, fuese uno de los dos elementos $n-2$, $p-1$, ó ambos, iguales á *cero*, conforme á la regla del caso 1.°, una ó dos veces aplicada, convertiríamos en positivos tambien todos los elementos, entre los que se hallan los dos expresados, excepto el primero. De todos modos, por lo tanto, es par la diferencia entre el número de los elementos sustituidos y el de los sustitutos; y la irregularidad se corre un lugar por lo ménos hácia la izquierda.

Cuando $\nu = -1$, la regla anterior no es aplicable; pero, si al mismo tiempo es $p > 1$, sumando y restando 2, tenemos:

$$(\mu,-1,p') = \mu + \frac{1}{-1+\frac{1}{p'}} = \mu - 2 - \frac{p'}{p'-1} + \frac{2(p'-1)}{p'-1} =$$

$$= \mu - 2 + \frac{p'-2}{p'-1} = \mu - 2 + \frac{1}{1+\frac{1}{p'-2}} = (\mu-2,1,p'-2)$$

y, por consecuencia:

$$(\mu,-1,p,q') = (\mu-2,1,p-2,q').$$

Si aquí fuese $p=2$, y entónces $p-2=0$, procederíamos con arreglo al método del caso 1.° Pero, si fuese $p=1$, tampoco podríamos usar esta fórmula; aunque entónces evidentemente:

$$(\mu, -1, 1, q') = \mu + \frac{1}{-1 + \frac{1}{1 + \frac{1}{q'}}} = \mu - 1 - q$$

y, por lo tanto:

$$(\mu, -1, 1, q, r, s') = (\mu - 2 - q, 1, r - 1, s').$$

Si aquí ocurriese ser $r = 1$, procederíamos como en el caso 1.°; y así continuaríamos.

Por tal procedimiento se consigue, en todos ellos sin excepcion, desviar la irregularidad de la fraccion dada un lugar, por lo ménos, hácia la izquierda; y se vé además que la diferencia, entre el número de los elementos variados y el de los elementos nuevos que los reemplazan, es siempre un número par. Aplicándole sucesivamente lograremos convertir la fraccion propuesta irregular

$$(\alpha, \beta, \gamma, \ldots \mu, \nu, p, q, r, \ldots t, u, v, \ldots)$$

en otra

$$(\alpha', b, c, \ldots k, l, u, v \ldots)$$

cuyos elementos todos, ménos el primero, sean números enteros y positivos: los cuales coincidirán con los de la fraccion primitiva, á contar desde uno determinado u, situado á distancia finita; siendo además un número *par* la diferencia entre el número de los elementos sustituidos

$$\alpha, \beta, \gamma, \ldots \mu, \nu, p, q, r \ldots t,$$

y el número de los sustitutos

$$\alpha', b, c, \ldots k, l,$$

segun hemos visto en todos los casos de trasformacion estudiados.

Verificada la trasformacion ó conversion expresada hasta aquí, pue-

de ocurrir que α' sea positivo, ó cero, ó un número negativo. En el primer supuesto, la conversion está completamente terminada, y el valor de la fraccion convertida es positivo; pero, si α' fuese negativo $=-a$, aquella fraccion sería negativa, é igual á la

$$-(a-1, 1, b-1, c.....):$$

ó, cuando $b=1$, á esta otra:

$$-(a-1, c+1, d, ...).$$

Y entónces se ve que el número de los elementos variados es menor, ó mayor, en una unidad, que el de los elementos nuevos por los cuales fueron aquéllos sustituidos: quedando así probado el último extremo de la proposicion al principio establecida.

f) Apoyados en las conclusiones anteriores, y en otros principios ya conocidos, vamos á demostrar ahora la siguiente:

Si entre cuatro números enteros $\alpha, \beta, \gamma, \delta$, *de los cuales sea el primero,* α, *diferente de cero, existe la relacion*

$$\alpha\delta - \beta\gamma = 1.$$

y entre otras dos cantidades ω *y* Ω, *la que sigue,*

$$\omega \quad \frac{\gamma + \delta\Omega}{\alpha + \beta\Omega}$$

se verificará tambien la igualdad

$$\omega = (\gamma', m, n, \ldots\ldots r, \beta', \Omega)$$

donde el número de los elementos enteros y positivos, $m, n, \ldots . r$, es par; y los dos γ', β', pueden tambien ser nulos, ó enteros negativos.

Para demostrarlo supondremos que α es positivo: lo cual no perjudica en nada á la generalidad que requiere el asunto; puesto que, si α fuera negativo, podríamos cambiar los signos de los cuatro enteros $\alpha, \beta, \gamma, \delta$; y este cambio no alteraria la dependencia establecida entre los mismos, y entre las dos cantidades ω y Ω.

Esto sentado, hagamos primeramente $\alpha = 1$. Entónces $\delta = \beta\gamma + 1$ é inmediatamente:

$$\omega = \frac{\gamma + (\beta\gamma + 1)\Omega}{1 + \beta\Omega} = \gamma + \frac{\Omega}{1 + \beta\Omega} = \gamma + \frac{1}{\beta + \dfrac{1}{\Omega}} = (\gamma, \beta, \Omega).$$

Y en este caso la proposicion es cierta.

Supongamos ahora $\alpha > 1$. Desarrollemos el quebrado $\gamma : \alpha$ en la fraccion contínua $(\gamma', m, n, \ldots . q, r)$, cuyos elementos son todos positivos, excepto el primero γ', que será positivo, nulo, ó negativo, segun que γ sea positivo y mayor que α, positivo y menor que α, ó finalmente, negativo; y hagamos siempre par, como podemos (*c*) el número de los elementos positivos $m, n, \ldots . r$. Desde luego será (*b*):

$$\frac{[\gamma', m, n, \ldots . q, r]}{[m, n, \ldots . q, r]} = \frac{\gamma}{\alpha};$$

y, como la reducida del primer miembro es un quebrado irreducible, y la fraccion generatriz $\gamma : \alpha$ es tambien irreducible, tendremos

$$\alpha = [m, n, \ldots . q, r] \qquad \text{y} \qquad \gamma = [\gamma', m, n, \ldots . q, r].$$

Por otra parte, como el número de los elementos $\gamma', m, n, \ldots . q, r$, es impar, se verifica la ley

$$[m, n, \ldots . q]\,[\gamma', m, n, \ldots . q, r] - [m, n, \ldots . q, r]\,[\gamma', m, n, \ldots . q] = -1;$$

y, por consecuencia, estas otras:

$$\alpha\,[\gamma', m, n, \ldots\ldots q] - [m, n, \ldots\ldots q]\,\gamma = 1 = \alpha\,\delta - \beta\,\gamma$$

de las cuales se desprenden (*b*):

$$\delta = [\gamma', m, n, \ldots\ldots q] + \gamma\,\beta'$$

$$\beta = [m, n, \ldots\ldots q] + \alpha\,\beta'$$

ó bien

$$\delta = [\gamma', m, n, \ldots\ldots q, r, \beta']$$

$$\beta = [m, n, \ldots\ldots q, r, \beta']$$

y, finalmente:

$$\frac{\delta}{\beta} = (\gamma', m, n, \ldots\ldots q, r, \beta').$$

Segun la ley de formacion de estas expresiones se verificarán tambien las igualdades

$$\gamma + \delta\,\Omega = [\gamma', m, n, \ldots\ldots q, r, \beta', \Omega]$$

$$\alpha + \beta\,\Omega = [m, n, \ldots\ldots q, r, \beta', \Omega]:$$

y, por lo tanto:

$$\frac{\gamma + \delta\,\Omega}{\alpha + \beta\,\Omega} = \omega = [\gamma', m, n, \ldots\ldots q, r, \beta', \Omega]$$

que es la que pretendíamos demostrar.

Réstanos advertir que, siendo las fracciones $\gamma : \alpha$ y $\beta : \alpha$ iguales respectivamente á las fracciones contínuas $(\gamma', m, n \ldots\ldots q, r)$ y $(\beta', r, q, \ldots\ldots m)$, los números γ' y β' son los máximos enteros, contenidos en aquéllas.

II.

Límite de una série infinita.

1.—*Caso particular.*

La proposicion, relativa á las séries llamadas *armónicas*, que procuramos demostrar aquí, es la siguiente:

Si a y b representan dos constantes positivas, la série infinita

$$S = \frac{1}{b^{1+\rho}} + \frac{1}{(b+a)^{1+\rho}} + \frac{1}{(b+2a)^{1+\rho}} + \frac{1}{(b+3a)^{1+\rho}} + \ldots\ldots$$

será convergente para todo valor de ρ, *tambien positivo; y, si este número* ρ *disminuye indefinidamente, el producto* ρS *se aproximará al límite* $\frac{1}{a}$.

En efecto: dado un valor (positivo) de ρ, construyamos la curva representada por la ecuacion

$$y = \frac{1}{x^{1+\rho}} \qquad (1)$$

referida á ejes rectangulares. El área de la superficie comprendida entre dicha línea y el eje de abscisas prolongado indefinidamente, á contar desde la abscisa determinada $x = b$, tendrá un valor finito, expresado por la integral

$$\int_b^{+\infty} y\,dx = \int_b^{+\infty} x^{-1+\rho}\,dx - \frac{1}{\rho\, b^{\rho}}. \qquad (2)$$

Las ordenadas de la curva (1), correspondiente á las abscisas

$$b,\quad b+a,\quad b+2a,\quad b+3a,\ldots..$$

son:

$$\frac{1}{b^{1+\rho}},\quad \frac{1}{(b+a)^{1+\rho}},\quad \frac{1}{(b+2a)^{1+\rho}},\quad \frac{1}{(b+3a)^{1+\rho}},\ldots..;$$

cuyos piés, equidistantes entre sí, dividen el eje de las x en un número infinito de trozos iguales todos á la constante a. Ahora bien, como las ordenadas sucesivas de la curva (1) van disminuyendo á medida que las abscisas crecen, sobre la base comun a podemos considerar dos séries de rectángulos: unos menores, y otros mayores que las superficies correspondientes, comprendidas entre la base comun a, y las dos ordenadas consecutivas hasta la curva solamente. Menores serán los rectángulos, siempre que por su altura tomemos la segunda ordenada de las dos consecutivas que lateralmente los limitan; y mayores, en el caso contrario: esto es, cuando por su altura tomemos la primera ordenada. La suma de las áreas de los rectángulos de la primera série, por consecuencia, será *menor* que el área (2) de la superficie comprendida entre el eje de abscisas, la curva y las dos ordenadas extremas; en signos:

$$\frac{a}{(b+a)^{1+\rho}} + \frac{a}{(b+2a)^{1+\rho}} + \frac{a}{(b+3a)^{1+\rho}} + \ldots.. < \frac{1}{\rho\, b^{\rho}},$$

ó bien, agregando á los dos miembros $\frac{a}{b^{1+\rho}}$:

$$a\,S < \frac{1}{\rho\, b^{\rho}} + \frac{a}{b^{1+\rho}}:$$

y esto prueba que la série S, formada sólo de términos positivos, es convergente para todo valor positivo de ρ.

La suma de las áreas de los rectángulos de la segunda série será *mayor* que la misma área (2), esto es:

$$\frac{a}{b^{1+\rho}} + \frac{a}{(b+a)^{1+\rho}} + \frac{a}{(b+2a)^{1+\rho}} + \ldots\ldots = aS > \frac{1}{\rho\, b^{\rho}}.$$

Y de uno y otro extremo se deduce que la série S, y, por lo tanto, el producto ρS, se halla comprendido entre dos límites, á saber:

$$\frac{1}{a\, b^{\rho}} < \rho S < \frac{1}{a\, b^{\rho}} + \frac{\rho}{b^{1+\rho}};$$

los cuales, cuando el valor positivo ρ disminuye indefinidamente, se aproximan á uno mismo, a^{-1}: que es tambien, en consecuencia, el límite á que se acerca dicho producto ρS.

2.—*Caso general.*

El teorema anterior es un caso particular del siguiente:

Designemos por K un sistema de números positivos k, y por T la funcion discreta, de una variable t, positiva y contínua, que expresa cuántos de los números k, contenidos en el sistema K, no exceden del valor de t. Cuando el cociente $T : t$, en el supuesto de crecer t indefinidamente, se aproxime á un límite finito y determinado, ω, la série

$$S = \Sigma \frac{1}{k^{1+\rho}}$$

será convergente, para todo valor positivo de ρ; y el producto ρS se aproximará al mismo límite ω, si ρ disminuye indefinidamente.

Detengámonos un poco á explicar este enunciado. Desde luego se colige; por lá significacion de T, que á todo valor finito de t habrá de corresponder otro, tambien finito, de aquella cantidad; porque, si existiera un conjunto infinito de números k, que no sobrepujasen al valor finito de t, á todo valor más grande de t corresponderia un número infinito T; y el cociente $T : t$, por consecuencia, seria entónces infinitamente grande: lo cual se halla en contradiccion con el supuesto establecido, de que tal cociente $T : t$, creciendo t, se aproxima á un límite finito ω. Y además es evidente que el número entero T variará tan sólo cuando adquiera t un valor, igual á uno, ó á varios, iguales entre sí, de los números k; y variará de pronto en tantas unidades cuantos números k existan iguales á dicho valor de t.

Si el sistema K se compusiera de un número finito de individuos k, fácilmente se probaria la exactitud del teorema enunciado; pues desde el momento en que llegara t á igualarse con el mayor de los números k, permaneceria T constante para todo crecimiento ulterior de t; el límite ω, de consiguiente, seria $T : \infty = 0$; y, como la suma

$$\Sigma \frac{1}{k}$$

tendria entónces un valor finito, el producto ρS, disminuyendo ρ indefinidamente, tendria tambien por límite 0.

Con igual sencillez se prueba que el caso particular, antes estudiado, se halla comprendido en el general que pretendemos demostrar ahora. En aquél se compone, en efecto, el sistema K de todos los números, $b+na$, correspondientes á todos los valores de $n=0, 1, 2, 3, \ldots\ldots$; y, como cualquiera que sea n, siempre podremos establecer las relaciones

$$b + n\,a \gtreqless t < b + (n + 1)\,a,$$

á las que corresponde el valor $T = n + 1$, resulta que el cociente $T : t$, creciendo t, y, por consecuencia, n, indefinidamente, se aproximará al límite

$$\omega = \frac{1}{a}:$$

el mismo que hallamos para el producto ρS, en el caso particular mencionado, bajo el supuesto de que el valor positivo ρ menguára indefinidamente.

Pasemos ya á la demostracion del teorema general. Con este fin ordénense, ante todo, segun su tamaño, y márquense con índices sucesivos, áun cuando haya varios de ellos iguales, los individuos k del sistema K, que formarán entónces la série

$$k_1 \leqq k_2 \leqq k_3 \leqq k_4 \leqq k_5 \ldots\ldots :$$

siempre realizable; por existir, debajo de un valor determinado de t, un número finito de los términos que la constituyen. Para referir ahora este caso general al particular, ya demostrado antes, y prescindiendo del que supone limitado el número de los elementos k, sin interés para nosotros, debemos probar que el cociente

$$h_n = \frac{n}{k_n} \qquad (1)$$

se aproxima tambien al límite ω, si n crece indefinidamente. Sea, pues, δ, una cantidad positiva, dada, tan pequeña como queramos; siempre hallaremos otra, tambien positiva, τ, correspondiente á la primera, de tal naturaleza que, para todos los valores $t \geqq \tau$, se verifique la condicion

$$\omega - \delta < \frac{T}{t} < \omega + \delta.$$

Designemos por ν el valor de T que corresponde al de $t = \tau$: ó, lo que es igual, sean

$$k_1, \quad k_2, \quad k_3, \ldots\ldots k_{\nu-1}, \quad k_\nu$$

todos los números k, contenidos en el sistema K, que no traspasan el valor τ; y por n cualquiera de los números enteros positivos $\nu + 1, \nu + 2, \nu + 3 \ldots\ldots$; entónces evidentemente será $k_n > \tau$; y, cuan-

do existan en el sistema K, varios individuos, iguales todos á k_n, tales como

$$k_{m+1}, \quad k_{m+2}, \ldots\ldots k_r,$$

n será igual tambien á cualquiera de los números $m+1, m+2, \ldots\ldots r$. Ahora bien, mientras el valor de t vaya creciendo desde k_m y aproximándose á k_n, permanecerá $T = m$, y el cociente $T : t$ irá disminuyendo y aproximándose al $m : k_n$: de lo cual se desprende, por ser $m < n$, que

$$\frac{T}{t} < k_n$$

mientras t permanezca, aunque muy poco, inferior á k_n; y, por el contrario, que

$$\frac{T}{t} \geq k_n,$$

cuando llegue á ser $T = r \geq n$. Mas en este crecimiento de la variable t, desde valores inferiores al k_n hasta igualarse con este número, mayor que τ, el cociente $T : t$ permanece siempre entre $\omega - \delta$ y $\omega + \delta$; y como, segun hemos visto, salta desde valores $< k_n$ hasta uno $\geq k_n$, tambien se verificará la condicion $\omega - \delta < k_n < \omega + \delta$. Luego, por diminuto que sea δ, siempre podrá elegirse n tan grande, que k_n se diferencie de ω en ménos todavía de lo que δ valga: esto es, k_n se aproximará al límite ω, cuando n crezca indefinidamente.

Esto sentado, desenvolvamos la série, que se desprende de la comprendida en la ecuacion (1):

$$S = \Sigma \frac{1}{k^{1+\rho}} = \frac{k_1^{1+\rho}}{1^{1+\rho}} + \frac{k_2^{1+\rho}}{2^{1+\rho}} + \frac{k_3^{1+\rho}}{3^{1+\rho}} + \ldots\ldots .$$

Si representamos por H la constante, bajo la cual permanece h_n, conforme acabamos de manifestar, áun cuando n crezca indefinidamente, la suma S', de los n primeros términos de la série última, será menor que el producto de $H^{1+\rho}$ por la suma s', de los n primeros términos de la que sigue:

$$s = \frac{1}{1^{1+\rho}} + \frac{1}{2^{1+\rho}} + \frac{1}{3^{1+\rho}} + \ldots\ldots;$$

y, como ésta es *convergente* para todo valor *positivo* de ρ (*caso* 1), *convergirá* tambien la otra S. Haciendo ahora $S = S' + S''$, $s = s' + s''$, y expresando por h simplemente el promedio (siempre positivo) de los valores $h_{n+1}, h_{n+2}, h_{n+3}, \ldots\ldots$, será $S'' = h^{1+\rho} s''$: luego, si tomamos n suficientemente grande (lo cual siempre es posible, por pequeña que sea δ) para que todos estos valores caigan entre $\omega - \delta$ y $\omega + \delta$, su promedio h, y tambien $h^{1+\rho}$ para un valor de ρ bastante pequeño, caerán entre dichos límites; y entre los mismos se hallará comprendido además el producto $\rho S'' = h^{1+\rho} . \rho s''$, en atencion á que $\rho s''$ converge hácia la unidad (*caso* 1) cuando ρ disminuye indefinidamente. Por otra parte, como S' comprende un número finito de términos, $\rho S'$ será infinitamente pequeño; y, por lo tanto, $\rho S = \rho S' + \rho S''$ tendrá los mismos límites laterales, $\omega - \delta$ y $\omega + \delta$, que $\rho S''$: de todo lo cual resulta finalmente que *el producto* ρS *converge hácia el límite* ω, *siempre que el de* ρ *sea* 0.

III.

Estudio de una ley geométrica.

Alguna semejanza guarda con lo dicho en el artículo precedente la proposicion geométrica que vamos á demostrar ahora, y cuyo enunciado es como sigue:

« Supongamos construida sobre un plano una figura F, limitada por todos sus frentes, de área A; y en el mismo dos ejes rectangulares, X é Y, y dos sistemas de rectas paralelas respectivamente á cada uno de ellos, y equidistantes todas entre sí. Expresando por δ la distancia comun entre las paralelas á los dos ejes, y por T el número de cruces ó puntos de la cuadrícula formada por ellas, que se hallen dentro del contorno finito F; el producto $T\delta^2$, disminuyendo δ indefinidamente, se aproximará al límite A. »

Fijémonos en el sistema de paralelas al eje Y; y, para mayor facilidad, admitamos que cada una de estas rectas corta dos veces solamente el contorno de la figura F. Si designamos por l la longitud del trozo, comprendido dentro de F, de una cualquiera de aquellas paralelas, será $l\delta$ la expresion aproximada del área de la parte de superficie F, limitada por dicho trozo y el de la paralela inmediata; y ya sabemos que la suma de todos estos rectángulos $l\delta$ (digámoslo así), ó elementos superficiales, segun las leyes de las cuadraturas, se aproxima al área total, A, si δ mengua indefinidamente. Representemos ahora por n el número de puntos de la cuadrícula que estén sobre el trozo l (incluyendo en él, ó no, los que caigan sobre el mismo contorno de la figura); es evidente que l se compondrá de $n-1$ partes iguales á δ, y de un resto que lo más llegará á 2δ: de modo que podremos establecer la igualdad $l = n\delta + \varepsilon\delta$, siendo ε un quebrado propio, positivo ó negativo; y multiplicándola por δ, escribir con razon:

$$\Sigma\, l\delta = \Sigma\,(n\delta^2 + \varepsilon\delta^2) = T\delta^2 + \delta\Sigma\,\varepsilon\delta.$$

Mas, como ε numéricamente puede valer á lo más 1; y la suma $\Sigma\varepsilon\delta$ podrá llegar, en consecuencia, cuando más valga tambien, á ser igual á la amplitud limitada de la figura F, en la direccion del eje de las X; la expresion $\delta\Sigma\varepsilon\delta$ será, simultáneamente con δ, infinitamente pequeña; y de resultas el producto $T\delta^2$ se aproximará, disminuyendo sin fin δ, al mismo límite que $\Sigma l\delta$, esto es: al área A; que es lo que pretendíamos demostrar.

Falta advertir que la ley anterior no se limita por la condicion, impuesta al sistema de las paralelas al eje Y, de cortar solamente en dos puntos el contorno de la figura F; pues no hay obstáculo para considerar ésta como conjunto de superficies parciales, positivas y negativas, mas sujetas todas á la condicion mencionada; y, aplicando entónces la ley demostrada á las partes separadamente, se logrará confirmar su exactitud respecto del todo.

IV.

Algunas proposiciones de Gauss referentes á su teoría de la division del círculo.

Cualquiera que sea la raiz representada por r (126-(2)), dice Gauss (*), siempre se verificarán las ecuaciones:

$$\Sigma[R] - \Sigma[N] = \pm\sqrt{p}, \text{ cuando } p \equiv 1 \pmod 4;$$

$$\Sigma[R] - \Sigma[N] = \pm i\sqrt{p}, \text{ cuando } p \equiv 3 \pmod 4:$$

en las cuales R y N expresan los restos y no-restos de p, inferiores á este módulo; y los símbolos $[R]$ y $[N]$ tienen la misma significacion que les dimos (128). Y, si k designa un número cualquiera, primo con p, tambien, como consecuencia de aquéllas, se verificarán estas otras:

$$\Sigma \cos\frac{R \cdot 2k\pi}{p} - \Sigma \cos\frac{N \cdot 2k\pi}{p} = \begin{cases} \pm\sqrt{p}, & \text{cuando } p \equiv 1 \pmod 4 \\ 0, & \text{cuando } p \equiv 3 \pmod 4 \end{cases}$$

$$\Sigma \operatorname{sen}\frac{R \cdot 2k\pi}{p} - \Sigma \operatorname{sen}\frac{N \cdot 2k\pi}{p} = \begin{cases} 0, & \text{cuando } p \equiv 1 \pmod 4 \\ \pm\sqrt{p}, & \text{cuando } p \equiv 3 \pmod 4 \end{cases}$$

Fácilmente se colige que estas sumas comprenden ciertas potencias de las raices (122-*b*) de la ecuacion del círculo (123) como sumandos. Gauss (**), antes que nadie, determinó el cuadrado de la siguiente:

(*) D. A. §. 356.

(**) Werke, t. II, pág. 23.

$$W = 1 + r + r^4 + r^9 + \ldots\ldots + r^{(p-1)^2},$$

mediante un procedimiento exclusivamente algebráico; pero Dirichlet, valiéndose del *Cálculo*, estudió con más generalidad y elegancia este asunto; y nosotros vamos á trasladar aquí, con la exactitud y claridad que podamos, las investigaciones de este ilustre matemático acerca del mismo, compendiadas hábilmente por Dedekind (*).

1.—*Lema concerniente á las séries de Fourier.*

En la teoría de estas séries se demuestra que, para los valores de x desde $x = 0$, hasta $x = \pi$ (estos límites inclusive), se verifica siempre la ecuacion

$$\varphi(x) = \frac{1}{2} a_0 + a_1 \cos x + a_2 \cos 2x + a_3 \cos 3x + \ldots\ldots \qquad (1)$$

cuando, dentro del expresado intervalo, representa $\varphi(x)$ una funcion contínua y finita; determinándose los coeficientes $a_0, a_1, a_2 \ldots\ldots$ por la fórmula

$$a_s = \frac{2}{\pi} \int_0^{\pi} \varphi(x) \cos s x \, d x:$$

de la cual, si suponemos $x = 0$, resulta esta otra:

$$\pi \varphi(0) = \sum_{-\infty}^{+\infty} \int_0^{\pi} \varphi(x) \cos s x \, d x:$$

(*) Dirichlet, *Zahlen-Theorie*, Suplemento I.

donde el signo sumatorio se refiere á la letra s que puede recibir sucesivamente todos los valores numéricos enteros, positivos y negativos, sin excluir tampoco el cero (*).

Establecida esta ley, consideremos ahora la integral más general

$$\int_0^{2h\pi} f(x) \cos s\,x\,dx$$

(*) Para determinar los coeficientes a_0, a_1, a_2, ... multiplíquense los dos miembros de la ecuacion (1) por $\cos s\,x\,dx$; é, integrando despues, se obtiene:

$$\int_0^{\pi} \varphi(x) \cos s\,x\,dx = \frac{1}{2} a_0 \int_0^{\pi} \cos\, s\,x\,dx + a_1 \int_0^{\pi} \cos x \cos s\,x\,dx + \ldots\ldots$$

Ahora bien, de las dos fórmulas conocidas:

$$\int \cos m\,x \cos s\,x\,dx = \frac{\cos m\,x \operatorname{sen} s\,x}{s} + \frac{m}{s} \int \operatorname{sen} m\,x \operatorname{sen} s\,x\,dx$$

$$\int \operatorname{sen} m\,x \operatorname{sen} s\,x\,dx = -\frac{\operatorname{sen} m\,x \cos s\,x}{s} + \frac{m}{s} \int \cos m\,x \cos s\,x\,dx,$$

se deduce:

$$\int \cos m\,x \cos s\,x\,dx = \frac{s \cos m\,x \operatorname{sen} s\,x - m \operatorname{sen} m\,x \cos s\,x}{s^2 - m^2}.$$

Esta integral, definida entre 0 y π, es igual á cero mientras m y s sean diferentes; pero, en el caso de que fuesen iguales m y s, tomaria la forma $0:0$, y su verdadero valor entónces se hallaria, como sabemos, sustituyendo por sus derivadas respecto á m los dos términos del segundo miembro, y haciendo en la nueva fraccion $m = s$. Procediendo así encontramos para valor de aquella integral, definida entre 0 y π, el quebrado $\pi:2$; con lo cual:

$$\int_0^{\pi} \varphi(x) \cos s\,x\,dx = a_s \cdot \frac{\pi}{2}.$$

en la que h representa un número entero, positivo, s un entero, positivo ó negativo, y $f(x)$ satisface á las mismas condiciones que $\varphi(x)$.

Esta integral, á condicion de que la letra r reciba los valores $0, 1, 2 \ldots\ldots 2h-1$, puede ser descompuesta en $2h$ integrales parciales de la forma

y de aquí se desprende la fórmula:

$$a_s = \frac{2}{\pi}\int_0^{\pi} \varphi(x)\cos s\,x\,dx,$$

que sirve para determinar los coeficientes a_0 , a_1 , a_2 , ... haciendo en ella respectivamente $s=0, 1, 2, \ldots\ldots$

La ecuacion (1) para $x=0$ se convierte en la

$$\varphi(0)=\frac{1}{2}a_0 + a_1 + a_2 + a_3 + \ldots\ldots$$

ó, aplicando la fórmula última, en la siguiente:

$$\varphi(0)=\frac{1}{\pi}\left(\int_0^{\pi}\varphi(x)\,dx+2\int_0^{\pi}\varphi(x)\cos x\,dx+2\int_0^{\pi}\varphi(x)\cos 2x\,dx+\ldots\ldots\right)$$

que puede escribirse abreviadamente:

$$\pi\,\varphi(0)=\sum_{-\infty}^{+\infty}\int_0^{\pi}\varphi(x)\cos s\,x\,dx.$$

En esta fórmula se refiere la sumacion á la letra s para todos los valores desde $-\infty$ hasta $+\infty$; porque sumar entre estos límites equivale á duplicar todos los términos, excepto el correspondiente á $s=0$, de la suma que se verificase desde 0 hasta $+\infty$.

$$\int_{r\pi}^{(r+1)\pi} f(x) \cos s\,x\,d\,x:$$

la cual, si tenemos en cuenta que su variable x puede ser sustituida por $(r\pi + x)$ ó $((r+1)\pi - x)$, segun r sea par ó impar, se convertirá en una de las dos siguientes:

$$\int_0^{\pi} f(r\pi + x) \cos s\,x\,d\,x \qquad \text{ó} \qquad \int_0^{\pi} f((r+1)\pi - x) \cos s\,x\,d\,x:$$

de donde, aplicando el lema anterior, se desprende:

$$\sum_{-\infty}^{\infty} \int_{r\pi}^{(r+1)\pi} f(x) \cos s\,x\,d\,x = \pi f(r\pi) \qquad \text{ó} \qquad = \pi f((r+1)\pi):$$

refiriéndose la letra s, en la suma del primer miembro, á todos los números enteros. Y, si damos ahora á la letra r sus valores $0, 1, 2, \ldots\ldots 2h-1$, y sumamos las ecuaciones resultantes, se obtiene finalmente la que sigue:

$$2\pi \left\{ \frac{1}{2} f(0) + f(2\pi) + f(4\pi) + \ldots\ldots + f(2(h-1)\pi) + \frac{1}{2} f(2h\pi) \right\}$$

$$= \sum_{-\infty}^{+\infty} \int_0^{2h\pi} f(x) \cos s\,x\,d\,x.$$

2. — *Valor de la suma* $\varphi(h, n)$ *cuando sea* $n \equiv 0 \,(mod.\ 4)$, *y* $h = 1$.

Estudiemos ahora las dos integrales

$$p = \int_{-\infty}^{+\infty} \cos\left(x^2\right) dx \quad \text{y} \quad q = \int_{-\infty}^{+\infty} \operatorname{sen}\left(x^2\right) dx.$$

Lo primero que debemos demostrar es que estas dos integrales representan valores finitos, determinados, áun cuando las funciones comprendidas bajo el signo de integracion no llegan á ser infinitamente pequeñas para valores infinitamente grandes de su variable x. Para esto trasformaremos las dos integrales propuestas, haciendo $x = \sqrt{y}$, en las siguientes:

$$p = 2\int_0^{\infty} \cos\left(x^2\right) dx = \int_0^{\infty} \frac{\cos y}{\sqrt{y}}\, dy$$

$$q = 2\int_0^{\infty} \operatorname{sen}\left(x^2\right) dx = \int_0^{\infty} \frac{\operatorname{sen} y}{\sqrt{y}}\, dy;$$

y de este modo se ve ya claro que, distribuyendo el desarrollo infinito de la integracion respecto de la variable positiva y, en grupos que contengan, cada uno, valores del mismo signo de la funcion integrable, las partes constituyentes de dicho desarrollo, que corresponden á los mencionados grupos, forman una série infinita, cuyos términos van alternando de signo y menguando todos indefinidamente, y es, por lo tanto, convergente.

Demostrado que las integrales p y q son finitas, pasemos á determinar sus valores numéricos. Designando, con este fin, por δ un ángulo cualquiera, constante, y haciendo por abreviar

$$p \cos \delta - q \operatorname{sen} \delta = \Delta,$$

dichas integrales pueden reunirse en una, á saber:

$$\Delta = \int_{-\infty}^{+\infty} \left(\cos \delta \cos \left(x^2 \right) - \operatorname{sen} \delta \operatorname{sen} \left(x^2 \right) \right) d x;$$

ó bien, son casos particulares de la siguiente:

$$\Delta = \int_{-\infty}^{+\infty} \cos \left(\delta + x^2 \right) d x = p \cos \delta - q \operatorname{sen} \delta:$$

la cual, si representamos además por α una constante cualquiera, y por $\sqrt{\alpha}$ su raiz *positiva;* y sustituimos por $x \sqrt{\alpha}$ la variable x, se convierte en esta otra:

$$\frac{\Delta}{\sqrt{\alpha}} = \int_{-\infty}^{+\infty} \cos \left(\delta + \alpha x^2 \right) d x:$$

donde habria que invertir los límites de la integracion en el caso de que $\sqrt{\alpha}$ fuese negativa. Introduzcamos una nueva constante β, y descompongamos la integral precedente en un número infinito de partes, de la forma

$$\int_{s\beta}^{(s+1)\beta} \cos \left(\delta + \alpha x^2 \right) d x,$$

en la que puede recibir la letra s todos los valores enteros desde $-\infty$ hasta $+\infty$. Esta última integral, á su vez, reemplazando x por $s\beta + x$, se reducirá á la siguiente:

$$\int_0^{\beta} \cos\left(\delta + \alpha s^2 \beta^2 + 2\alpha s \beta x + \alpha x^2\right) dx.$$

Si definimos las constantes positivas α y β, hasta ahora completamente arbitrarias, por las ecuaciones

$$\alpha \beta^2 = 2m\pi, \qquad 2\alpha\beta = 1,$$

siendo m un entero cualquiera positivo, tendremos desde luego:

$$\beta = 4m\pi, \qquad \alpha = \frac{1}{8m\pi}.$$

y tambien:

$$\cos\left(\delta + \alpha s^2 \beta^2 + 2\alpha s \beta x + \alpha x^2\right) = \cos\left(\delta + s x + \alpha x^2\right):$$

en atencion á que, siendo s un número entero, $s^2 \alpha \beta^2 = s^2 2m\pi$ representa un múltiplo de la circunferencia; y, sustituyendo α por su nuevo valor,

$$\cos\left(\delta + \alpha x^2 + s x\right) = \cos\left(\delta + \frac{x^2}{8m\pi}\right)\cos s x - \operatorname{sen}\left(\delta + \frac{x^2}{8m\pi}\right)\operatorname{sen} s x;$$

de lo cual resulta:

$$\int_{s\beta}^{(s+1)\beta} \cos\left(\delta + \alpha x^2\right) dx$$

$$= \int_0^{4m\pi} \cos\left(\delta + \frac{x^2}{8m\pi}\right)\cos s x\, dx - \int_0^{4m\pi} \operatorname{sen}\left(\delta + \frac{x^2}{8m\pi}\right)\operatorname{sen} s x\, dx.$$

Pero la segunda integral del segundo miembro de esta ecuacion, por contener el factor $\operatorname{sen} s\,x$, desaparece evidentemente para $s = 0$, y adquiere valores iguales y de signo contrario para cada dos valores, tambien iguales y de signo contrario, de s: luego, efectuando la suma de todos los valores que tome dicha ecuacion, correspondientes á todos los de s, desde $-\infty$ hasta $+\infty$, será:

$$\frac{\Delta}{\sqrt{\alpha}} = \Delta\sqrt{8\,m\,\pi} = \sum_{-\infty}^{+\infty} \int_{0}^{4m\pi} \cos\left(\delta + \frac{x^2}{8\,m\,\pi}\right) \cos s\,x\,d\,x.$$

Ya estamos en aptitud de aplicar la última fórmula del artículo anterior, cuyo segundo miembro coincidirá con el de la ecuacion inmediata, haciendo en ésta

$$f(x) = \cos\left(\delta + \frac{x^2}{8\,m\,\pi}\right) \qquad y \qquad h = 2\,m.$$

De la aplicacion de la fórmula recordada resulta esta otra:

$$\Delta\sqrt{8\,m\,\pi} = 2\,\pi\left\{\frac{1}{2}f(0) + f(2\pi) + \ldots\ldots + f(2\,(2m-1)\,\pi) + \frac{1}{2}f(4\,m\,\pi)\right\}$$

en la cual deberá tomarse $\sqrt{8\,m\,\pi} = \dfrac{1}{\sqrt{\alpha}}$ *positivamente*. Para modificarla establezcamos la igualdad

$$f(4\,m\,\pi + 2\,s\,\pi) = f(2\,s\,\pi).$$

evidente por representar s un entero cualquiera, y ser así

$$\cos\left(\delta+\frac{(4m\pi+2s\pi)^2}{8\,m\,\pi}\right)=\cos\left(\delta+\frac{(2s\pi)^2}{8\,m\,\pi}+2\pi\,(m+s)\right)=$$

$$=\cos\left(\delta+\frac{(2s\pi)^2}{8m\pi}\right)=f\,(2\,s\,\pi).$$

De ella se desprende que:

$$f\,(2\,s\,\pi)=\tfrac{1}{2}f\,(2\,s\,\pi)+\tfrac{1}{2}f\left(2\,(2\,m+s)\,\pi\right);$$

y dando ahora á s los valores $0, 1, 2, \ldots\ldots 4\,m-1$, que representan un sistema completo de restos (mod. $4\,m$), se advertirá claramente que la suma, inclusa en el paréntesis de la fórmula que tratamos de modificar, puede ser expresada simbólicamente por

$$\tfrac{1}{2}\sum f\,(2\,s\,\pi).$$

Introduciendo, pues, este nuevo símbolo en aquella fórmula, y no olvidando que la variable x es ahora $2\,s\,\pi$, obtendremos la siguiente:

$$\Delta\sqrt{8\,m\,\pi}=\pi\sum\cos\left(\delta+s.^2\,\frac{2\pi}{n}\right).$$

De acuerdo con el epígrafe de este artículo hagamos ahora $4m=n$, esto es, designemos por n un entero cualquiera, positivo, mas divisible por 4; y por $\sqrt{n}$ y $\sqrt{\tfrac{1}{2}\pi}$ las raices cuadradas *positivas* de n y de $\tfrac{1}{2}\pi$; la última expresion tomará la nueva forma:

$$\Delta \sqrt{n} = \sqrt{\tfrac{1}{2}\pi} \cdot \sum \cos\left(\delta + s^2 \frac{2\pi}{n}\right);$$

donde la letra s puede recibir los valores de cualquier sistema completo de restos (mod. n). Por otra parte tenemos:

$$\Delta = p \cos\delta - q \operatorname{sen}\delta,$$

representando p y q, como sabemos, valores finitos de integrales que son independientes de n y δ. Haciendo, pues, primeramente $n = 4$, que es la más simple de las suposiciones que pueden sentarse, conformes con las condiciones de n, se halla:

$$\Delta \cdot 2 = \sqrt{\tfrac{1}{2}\pi}\left\{\cos\delta + \cos\left(\delta + \frac{\pi}{2}\right) + \cos(\delta + 2\pi) + \cos\left(\delta + 4\pi + \frac{\pi}{2}\right)\right\}$$

ó bien:

$$2\,(p\cos\delta - q\operatorname{sen}\delta) = 2\,(\cos\delta - \operatorname{sen}\delta)\sqrt{\tfrac{1}{2}\pi};$$

y atribuyendo ahora á la arbitraria δ los valores sucesivos 0 y $\frac{1}{2}\pi$, resulta:

$$p = q = \sqrt{\tfrac{1}{2}\pi}.$$

Determinados así p y q, la ecuacion que principalmente estudiamos se reduce á la siguiente:

$$\sum \cos\left(\delta + s^2 \frac{2\pi}{n}\right) = (\cos\delta - \operatorname{sen}\delta)\sqrt{n}$$

que se descompone en las dos:

$$\sum \cos\left(s^2 \frac{2\pi}{n}\right) = \sqrt{n}$$

$$\sum \operatorname{sen}\left(s^2 \frac{2\pi}{n}\right) = \sqrt{n},$$

significando en ellas n un múltiplo positivo de 4, y $\sqrt{n}$ la raiz *positiva* de n. Y éstas, á su vez, representando, como siempre, por i la raiz $\sqrt{-1}$, y por e la base de los logaritmos neperianos, se compendian finalmente en la simbólica:

$$\sum e^{s^2 \frac{2\pi i}{n}} = (1+i)\sqrt{n};$$

donde s, puede recibir los valores de un sistema completo de restos, segun el módulo n.

3.—*Leyes generales de las sumas* $\varphi(h, n)$.

Desechando las restricciones impuestas en el artículo precedente á los números n y h, supongamos ahora que n sea un número entero cualquiera, positivo, y h un entero, tambien cualquiera, mas positivo ó negativo; y escribamos abreviadamente:

$$\sum e^{s^2 \frac{2h\pi i}{n}} = \varphi(h, n),$$

conservando s su anterior significado. Es claro que, con la nueva notacion, la ley particular, antes demostrada, podrá expresarse como sigue:

$$\varphi(1, n) = (1+i)\sqrt{n}, \quad \text{cuando } n \equiv 0 \pmod 4.$$

Mas esta suma particular, y otras varias, se hallan comprendidas en la anterior $\varphi(h, n)$, cuyas propiedades generales vamos á estudiar seguidamente.

1.ª *Si es* $h \equiv h' \ (mod.\ n)$, *será tambien*

$$\varphi(h, n) = \varphi(h', n).$$

Porque para todo valor entero de s siempre se verifica la igualdad

$$e^{s^2 \frac{2h\pi i}{n}} = e^{s^2 \frac{2h'\pi i}{n}}$$

2.ª *Si* a *es primo con* n, *será tambien*

$$\varphi(h a^2, n) = \varphi(h, n).$$

Pues evidentemente:

$$\varphi(h a^2, n) = \sum e^{as_j{}^2 \frac{2h\pi i}{n}};$$

y cuando s recorra un sistema completo de restos (mod. n), el producto as lo recorrerá (63) tambien.

3.ª *Si* m *y* n *son números primos entre sí, y ambos positivos, será*

$$\varphi(hm, n)\, \varphi(hn, m) = \varphi(h, mn).$$

En efecto:

$$\varphi(hm, n) = \sum e^{s^2 \frac{2hm\pi i}{n}}; \qquad \varphi(hn, m) = \sum e^{t^2 \frac{2hn\pi i}{m}}$$

representando las letras s y t un sistema completo de restos, cada una, segun los módulos n y m respectivamente; y, por consecuencia:

$$\varphi(hm, n)\, \varphi(hn, m) = \sum e^{\left(\frac{ms^2}{n} + \frac{nt^2}{m}\right) 2h\pi i}$$

refiriéndose el signo sumatorio á todas las mn combinaciones de cada uno de los valores de s con cada uno de los valores de t. Ahora bien, como

$$\frac{m\,s^2}{n} + \frac{n\,t^2}{m} = \frac{(m\,s + n\,t)^2}{m\,n} - 2\,s\,t,$$

y todos los múltiplos de $2\pi i$ pueden suprimirse en el exponente de e, tendremos:

$$\varphi(h\,m, n)\,\varphi(h\,n, m) = \sum e^{(ms+nt)^2 \frac{2h\pi i}{m\,n}}.$$

Mas, si establecemos la igualdad

$$m\,s + n\,t = r,$$

se concibe bien pronto que, cuando s y t hayan recibido todos sus valores, habrá adquirido r tambien $m\,n$ valores, incongruentes todos segun el módulo mn; pues de la congruencia evidente, dada la significacion de s y t,

$$m\,s + n\,t \equiv m\,s' + n\,t' \text{ (mod. } mn),$$

se desprenden estas otras:

$$m\,s \equiv m\,s' \text{ (mod. } n), \qquad n\,t \equiv n\,t' \text{ (mod. } m):$$

y, por ser m y n primos entre sí, las siguientes:

$$s \equiv s' \text{ (mod } n), \qquad t \equiv t' \text{ (mod. } m):$$

las cuales patentizan que sólo podrá adquirir r valores congruentes (mod. mn), cuando los valores de s sean congruentes (mod. n), y los de t congruentes (mod. m); y por consecuencia, que á las mn combinaciones diferentes de los valores de s y t, corresponden mn valores de r, incongruentes (mod. $m\,n$), que constituyen un sistema completo de restos segun este módulo $m\,n$: luego

$$\varphi(h\,m, n)\,\varphi(h\,n, m) = \sum e^{r^2 \frac{2h\pi i}{mn}} = \varphi(h, m\,n);$$

que era lo que pretendíamos demostrar.

4. — *Determinacion general de la suma* $\varphi(1, n)$.

El valor de la suma $\varphi(1, n)$, hallado antes para el caso particular $n \equiv 0 \pmod 4$, puede ahora determinarse, respecto de cualquiera otro valor de n, con auxilio de las leyes que acabamos de demostrar en el artículo precedente.

Supongamos desde luego que n sea un número cualquiera, pero *impar*. Haciendo en la ley 3.ª de las mencionadas,

$$h = 1, \quad m = 4.$$

tendremos:

$$\varphi(4, n)\,\varphi(n, 4) = \varphi(1, 4\,n).$$

Conforme á la ley 2.ª,

$$\varphi(4, n) = \varphi(2^2, n) = \varphi(1, n);$$

por otra parte:

$$\varphi(n, 4) = \sum e^{s^2 \frac{2n\pi i}{4}} = \sum e^{s^2 \frac{n\pi i}{2}} = e^0 + e^{\frac{n\pi i}{2}} + e^{2n\pi i} + e^{\frac{9n\pi i}{2}} -$$

$$= 1 + i^n + 1 + i^n = 2\,(1 + i^n);$$

y, de acuerdo con la ley (2):

$$\varphi(1, 4n) = (1+i)\sqrt{4n} = 2(1+i)\sqrt{n};$$

luego

$$\varphi(1, n) \cdot 2(1+i^n) = 2(1+i)\sqrt{n},$$

de donde:

$$\varphi(1, n) = \frac{1+i}{1+i^n}\sqrt{n}.$$

Ahora bien, segun sea $n \equiv 1$, ó $\equiv 3 \pmod 4$, así será

$$i^n = i, \quad \text{ó} \quad = -i;$$

y, en consecuencia:

$$\frac{1+i}{1+i^n} = 1, \quad \text{ó} \quad = \frac{1+i}{1-i} = i;$$

y finalmente:

$$\varphi(1, n) = \sqrt{n} \quad \text{ó} \quad = i\sqrt{n};$$

pudiéndose compendiar estos dos resultados en la única fórmula:

$$\varphi(1, n) = i^{\frac{1}{4}(n-1)^2}\sqrt{n}.$$

Supongamos ahora que n sea *par*, mas no múltiplo de 4 (caso ya estudiado (2)), sino duplo de un número impar. En la citada ley 3.ª del artículo anterior haremos

$$h = 1, \quad m = 2,$$

y pondremos $\frac{1}{2}n$ por n, para que se realicen todas las condiciones que la misma exije; será, pues:

$$\varphi(2, \tfrac{1}{2}n)\,\varphi(\tfrac{1}{2}n, 2) = \varphi(1, n);$$

y, como

$$\varphi(\tfrac{1}{2}n, 2) = \sum e^{s^2 \frac{n\pi i}{2}} = e^0 + e^{\frac{n\pi i}{2}} = 1 - 1 = 0,$$

resulta por último:

$$\varphi(1, n) = 0.$$

En suma:

$$\varphi(1, n) = (1 + i\sqrt{n}), \qquad \text{cuando } n \equiv 0 \pmod 4$$

$$\varphi(1, n) = i^{\frac{1}{4}(n-1)^2}\sqrt{n} \quad \ldots\ldots \quad n \equiv 1 \pmod 2$$

$$\varphi(1, n) = 0 \quad \ldots\ldots \quad n \equiv 2 \pmod 4$$

5.—*Determinacion general de* $\varphi(h, n)$.

Vamos á determinar ahora el valor de la suma $\varphi(h, n)$, para cualquier valor de h, mas imponiendo al número n la condicion ó limitacion de ser impar. Designemos este número impar por p; por α sus $\frac{1}{2}(p-1)$ restos incongruentes, y por β sus $\frac{1}{2}(p-1)$ no-restos; entónces

$$\varphi(h, p) = \sum e^{s^2 \frac{2h\pi i}{p}} = 1 + 2\sum e^{\alpha \frac{2h\pi i}{p}};$$

puesto que, si atribuimos á s los valores de un sistema completo de

restos (mod. p), sus cuadrados s^2 son congruentes entre sí dos á dos, y con los α restos cuadráticos de p (104); esceptuando el 0 para el cual es $e^0 = 1$. Mas por otra parte

$$1 + \sum e^{\alpha \frac{2h\pi i}{p}} + \sum e^{\beta \frac{2h\pi i}{p}} = \sum e^{s \frac{2h\pi i}{p}} = 0;$$

en atencion á que, mientras h no sea divisible por p, el símbolo

$$\sum e^{s \frac{2h\pi i}{p}}$$

representa la suma de las raices de una ecuacion binomia de grado p: luego, sustituyendo en la ecuacion primera el valor de

$$1 + \sum e^{\alpha \frac{2h\pi i}{p}} = -\sum e^{\beta \frac{2h\pi i}{p}}$$

deducido de la última, hallamos:

$$\varphi(h, p) = \sum e^{\alpha \frac{2h\pi i}{p}} - \sum e^{\beta \frac{2h\pi i}{p}};$$

y como, empleando el símbolo de Legendre,

$$e^{\alpha \frac{2h\pi i}{p}} = \left(\frac{\alpha}{p}\right) e^{\alpha \frac{2h\pi i}{p}} \quad \text{y} \quad -e^{\beta \frac{2h\pi i}{p}} = \left(\frac{\beta}{p}\right) e^{\beta \frac{2h\pi i}{p}},$$

será finalmente:

$$\varphi(h, p) = \sum e^{\alpha \frac{2h\pi i}{p}} - \sum e^{\beta \frac{2h\pi i}{p}} = \sum \left(\frac{s}{p}\right) e^{s \frac{2h\pi i}{p}},$$

donde s puede recibir los valores $1, 2, 3, \ldots\ldots p-1$. Esta última expresion puede modificarse todavía. Recordando (104) que

$$\left(\frac{hs}{p}\right) = \left(\frac{h}{p}\right)\left(\frac{s}{p}\right), \quad \text{y que} \quad \left(\frac{h}{p}\right)\left(\frac{h}{p}\right) = 1,$$

puede, en efecto, convertirse en esta otra:

$$\varphi(h, p) = \left(\frac{h}{p}\right) \sum \left(\frac{hs}{p}\right) e^{hs \frac{2\pi i}{p}},$$

ó bien, en la siguiente:

$$\varphi(h, p) = \left(\frac{h}{p}\right) \sum \left(\frac{s}{p}\right) e^{s \frac{2\pi i}{p}};$$

en virtud de que, no siendo h divisible por p, la letra s y el producto hs recorren simultáneamente un sistema completo de restos (con excepcion del número $\equiv 0$), segun el módulo p.

Haciendo ahora $h=1$, hallamos:

$$\varphi(1, p) = \sum \left(\frac{s}{p}\right) e^{s \frac{2\pi i}{p}},$$

y de consiguiente (4):

$$\varphi(h, p) = \left(\frac{h}{p}\right) \varphi(1, p) = \left(\frac{h}{p}\right) i^{\frac{1}{4}(p-1)^2} \sqrt{p},$$

debiéndose tomar siempre $\sqrt{p}$ positiva.

Si h es divisible por p, de la misma definicion de estas sumas se deduce inmediatamente:

$$\varphi(h, p) = p.$$

Mediante el último resultado, y la ley 3.ª del artículo (3), se puede demostrar fácilmente la ley de reciprocidad entre dos números primos, impares y positivos, p y q. En efecto, de acuerdo con dicho resultado, tenemos:

$$\varphi(q, p) = \left(\frac{q}{p}\right) i^{\frac{1}{4}(p-1)^2} \sqrt{p}$$

$$\varphi(p, q) = \left(\frac{p}{q}\right) i^{\frac{1}{4}(q-1)^2} \sqrt{q};$$

y, segun la ley citada:

$$\varphi(q, p)\, \varphi(p, q) = \varphi(1, p\, q).$$

Mas (4):

$$\varphi(1, p\, q) = i^{\frac{1}{4}(p\, q-1)^2} \sqrt{p\, q},$$

siendo

$$\sqrt{p\, q} = \sqrt{p} \cdot \sqrt{q}:$$

luego

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) i^{\frac{1}{4}(p-1)^2 + \frac{1}{4}(q-1)^2} \sqrt{p} \cdot \sqrt{q} = i^{\frac{1}{4}(p\, q-1)^2} \sqrt{p\, q}.$$

y, por consecuencia:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = i^{\lambda};$$

habiendo escrito el exponente λ, en obsequio á la brevedad, en vez de la expresion

$$\frac{(pq-1)^2-(p-1)^2-(q-1)^2}{4} = \frac{p-1}{2} \cdot \frac{q-1}{2} \left\{(p+1)(q+1)-2\right\}.$$

Y, como evidentemente se verifica la congruencia

$$(p+1)(q+1)-2 \equiv 2 \,(\text{mod. } 4),$$

resulta por último la ecuacion

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = i^{\frac{1}{2}(p-1)(q-1)} = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)},$$

que expresa la *ley de reciprocidad* (115).

Con igual sencillez, basados en los mismos principios, podríamos demostrar casi todos los teoremas referentes á los restos cuadráticos: mas ésto nos apartaria de nuestro propósito.

6.— *Demostracion de una fórmula empleada en los artículos* (176) *y* (177) *del texto.*

—

En la hipótesis de ser p un número primo impar, y h un entero cualquiera, no divisible por p, hemos encontrado en el artículo precedente la fórmula que sigue:

$$\sum\left(\frac{s}{p}\right) e^{s\frac{2h\pi i}{p}} = \left(\frac{h}{p}\right)\varphi(1,p);$$

ó bien, poniendo por $\varphi(1,p)$ su valor, ya conocido:

$$\sum\left(\frac{s}{p}\right) e^{s\frac{2h\pi i}{p}} = \left(\frac{h}{p}\right) i^{\frac{1}{4}(p-1)^2}\sqrt{p}: \qquad (1)$$

en la cual, si ha de comprender tambien el caso exceptuado en que $h \equiv 0 \pmod{p}$, debemos hacer

$$\left(\frac{h}{p}\right) = 0,$$

siempre que h sea divisible por p; porque, en tal supuesto, se reduce su primer miembro á

$$\sum\left(\frac{s}{p}\right) = 0,$$

por ser el número de restos igual al de no-restos. Y, extendiendo este resultado, referente al símbolo de Legendre, al definido por Jacobi (118), podremos asimismo establecer la igualdad

$$\left(\frac{m}{P}\right) = 0,$$

siempre que m no sea primo con P.

La ecuacion (1) es general para todo número primo impar, positivo, p, y cualquier entero h, pudiendo abrazar tambien la suma que constituye su primer miembro la clase de números $s \equiv 0 \,(\text{mod. } p)$. Vamos á demostrar ahora que todavía puede dicha ley (1), en igual forma, abarcar los números compuestos, con tal que sean impares y no divisibles por ningun cuadrado (excepto el 1). Designemos por

$$P = pp'p''.....$$

uno de tales números, cuyos factores $p, p', p''.....$ serán números primos impares, diferentes; y establezcamos para mayor facilidad las igualdades:

$$\frac{P}{p} = Q, \quad \frac{P}{p'} = Q', \quad \frac{P}{p''} = Q'', ...$$

Aplicando la ecuacion (1) á los factores $p, p', p''.....$ sucesivamente, hallaremos estas otras:

$$\sum \left(\frac{s}{p}\right) e^{s\frac{2h\pi i}{p}} = \left(\frac{h}{p}\right) i^{\frac{1}{4}(p-1)^2} \sqrt{p}$$

$$\sum \left(\frac{s'}{p'}\right) e^{s'\frac{2h\pi i}{p}} = \left(\frac{h}{p'}\right) i^{\frac{1}{4}(p'-1)^2} \sqrt{p'}$$

$$\sum \left(\frac{s''}{p''}\right) e^{s''\frac{2h\pi i}{p}} = \left(\frac{h}{p''}\right) i^{\frac{1}{4}(p''-1)^2} \sqrt{p''}$$

.....

.....

de las que, haciendo por abreviar,

$$s\,Q + s'\,Q' + s''\,Q'' + \ldots\ldots = m,$$

y, teniendo en cuenta (118) que

$$\left(\frac{h}{p}\right)\left(\frac{h}{p'}\right)\left(\frac{h}{p''}\right)\ldots\ldots = \left(\frac{h}{P}\right),$$

se deduce por multiplicacion la siguiente:

$$\sum\left(\frac{s}{p}\right)\left(\frac{s'}{p'}\right)\left(\frac{s''}{p''}\right)\ldots\ldots e^{m\frac{2h\pi i}{P}} = \left(\frac{h}{P}\right) i^{\frac{1}{4}(p-1)^2 + \frac{1}{4}(p'-1)^2 + \frac{1}{4}(p''-1)^2 + \ldots\ldots}\sqrt{P}. \tag{2}$$

donde $\sqrt{P}$ se toma positivamente, y el signo sumatorio se refiere á todas las $p\,p'\,p''\ldots\ldots = P$ combinaciones de todos los valores de $s, s', s''\ldots\ldots$ Desde luego se concibe que á cada dos de estas combinaciones, diferentes, corresponden tambien dos valores diferentes de m; pues, si estos valores de m no lo fueran, y se verificara, entónces, la congruencia

$$s\,Q + s'\,Q' + s''\,Q'' + \ldots\ldots \equiv s\,Q + t'\,Q' + t''\,Q'' + \ldots\ldots \pmod{P},$$

como los cocientes $Q', Q'', \ldots\ldots$ son todos divisibles por p, se verificaria tambien esta otra:

$$s\,Q \equiv t\,Q \pmod{p};$$

y asimismo la que sigue:

$$s \equiv t \pmod{p},$$

por ser Q primo con p; é igualmente las que se desprenden del mismo supuesto: $s' \equiv t' \pmod{p'}$, $s'' \equiv t'' \pmod{p''}$ ..... Lo cual quiere decir que dos valores congruentes de m exigen tambien dos combina-

ciones, $s'\,s', s''$ ..... y t, t', t'' ....., idénticas; y, en consecuencia, que m representa ó recorre un sistema completo de restos segun el módulo P. Por otra parte:

$$\left(\frac{m}{p}\right)=\left(\frac{s\,Q+s'\,Q'+s''\,Q''+\ldots..}{p}\right)=\left(\frac{s\,Q}{p}\right)=\left(\frac{s}{p}\right)\left(\frac{Q}{p}\right),$$

y del mismo modo:

$$\left(\frac{m}{p'}\right)=\left(\frac{s'}{p'}\right)\left(\frac{Q'}{p'}\right),\qquad \left(\frac{m}{p''}\right)=\left(\frac{s''}{p''}\right)\left(\frac{Q''}{p''}\right),\ldots..;$$

y multiplicando todas estas ecuaciones ordenadamente:

$$\left(\frac{m}{P}\right)=\left(\frac{s}{p}\right)\left(\frac{s'}{p'}\right)\left(\frac{s''}{p''}\right)\ldots..\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\ldots..$$

Mediante esta ecuacion, y la (2) multiplicada por

$$\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\ldots..,$$

se obtiene la que sigue:

$$\sum\left(\frac{m}{P}\right)e^{m\frac{2h\pi i}{P}}=\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\ldots..\left(\frac{h}{P}\right)i^{\Sigma\frac{1}{4}(p-1)^2}\sqrt{P},$$

en cuyo segundo miembro hemos hecho por abreviar:

$$\tfrac{1}{4}(p-1)^2+\tfrac{1}{4}(p'-1)^2+\tfrac{1}{4}(p''-1)^2+\ldots..=\Sigma\tfrac{1}{4}(p-1)^2.$$

Además, segun el símbolo de Jacobi:

$$\left(\frac{Q}{p}\right) = \left(\frac{p'}{p}\right)\left(\frac{p''}{p}\right)\ldots\ldots$$

$$\left(\frac{Q'}{p'}\right) = \left(\frac{p}{p'}\right)\left(\frac{p''}{p'}\right)\ldots\ldots$$

$$\left(\frac{Q''}{p''}\right) = \left(\frac{p}{p''}\right)\left(\frac{p'}{p''}\right)\ldots\ldots$$

y, por consecuencia:

$$\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\ldots\ldots = \Pi\left(\frac{p}{p'}\right)\left(\frac{p'}{p}\right),$$

refiriéndose el signo-producto Π á todos los pares posibles de factores primos, diferentes, tales como p y p'. Mas, segun la ley de reciprocidad, es

$$\left(\frac{p}{p'}\right)\left(\frac{p'}{p}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(p'-1)} = i^{-\frac{1}{2}(p-1)(p'-1)};$$

y generalizando:

$$\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\ldots\ldots = i^{2\Sigma\frac{1}{2}(p-1)\cdot\frac{1}{2}(p'-1)},$$

refiriéndose el signo-sumatorio aquí tambien á todos los pares posibles, p, p', de factores primos diferentes. Y evidentemente:

$$\Sigma\,\tfrac{1}{4}(p-1)^2 + 2\Sigma\,\tfrac{1}{2}(p-1)\cdot\tfrac{1}{2}(p'-1) =$$

$$= \left(\tfrac{1}{2}(p-1) + \tfrac{1}{2}(p'-1) + \tfrac{1}{2}(p''-1) + \ldots\ldots\right)^2$$

Luego

$$\sum \left(\frac{m}{P}\right) e^{m\frac{2h\pi i}{P}} = \left(\frac{h}{p}\right) i^{\left[\frac{1}{2}(p-1)+\frac{1}{2}(p'-1)+\ldots\ldots\right]^2} \sqrt{P};$$

ecuacion que, mediante la congruencia ya conocida (119)

$$\frac{P-1}{2} \equiv \frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} + \ldots\ldots \pmod 2$$

y su consiguiente

$$\left(\frac{P-1}{2}\right)^2 \equiv \left(\frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} + \ldots\ldots\right)^2 \pmod 4,$$

se convierte, por fin, en esta otra:

$$\sum \left(\frac{m}{P}\right) e^{m\frac{2h\pi i}{P}} = \left(\frac{h}{P}\right) i^{\frac{1}{4}(P-1)^2} \sqrt{P};$$

que es, en efecto, la que pretendíamos demostrar.

Si en ella suponemos, como anteriormente, $h \equiv 0 \pmod P$, se obtiene de nuevo la ley (121—I)

$$\sum \left(\frac{m}{P}\right) = 0.$$

V.

Sobre los sistemas de numeracion y la divisibilidad de los números.

1.—*Expresion de un número en sistemas diferentes de numeracion.*

Suponiendo conocido lo que se entiende por sistemas de numeracion, y las reglas de las operaciones fundamentales de la Aritmética en cualquier sistema (*), el problema que tratamos de resolver ahora es el siguiente:

Dado un número, escrito en un sistema de numeracion, hallar su expresion en otro sistema.

Para conseguirlo se nos ofrecen dos caminos distintos: 1.° ejecutar las operaciones necesarias con arreglo al nuevo sistema; 2.° ejecutarlas conforme al antiguo: lo cual exije ante todo: ó que se conozca la base antigua en el nuevo sistema, ó la base nueva en el sistema antiguo.

Sea, pues,

$$N_b = a_{n-1}\, b^{n-1} + \ldots\ldots + a_1 b + a_0 = a_{n-1} \ldots\ldots a_2\, a_1\, a_0 \qquad (1)$$

el número, de n cifras, escrito en el sistema regular, ó de base constante b, el que tratamos de expresar en el sistema tambien regular, de base b'.

1.° Escríbase la base antigua b en el nuevo sistema; y, como en

(*) Véanse las *Lecciones de Aritmética* por D. Ambrosio Moya, pág. 129 y siguientes.

este mismo se conocerán tambien las cifras a, determinaremos los productos respectivos de estas cifras por las potencias sucesivas de la base, y sumaremos despues tales productos para obtener el número N_b escrito en el sistema que se pide: todo conforme manifiesta la igualdad (1).

2.° Escríbase la base nueva, b', en el sistema antiguo; y por esta base, así escrita, divídase despues el número dado N_b, y los cocientes sucesivos; los restos sucesivos y el último cociente serán los valores de las cifras a' en el nuevo sistema, y en el mismo órden que van obteniéndose.

Puesto que la base menor es conocida siempre, y tiene una sola cifra en el sistema de base mayor, siempre será posible ejecutar en éste las operaciones para resolver el problema de que se trata; mas, si uno de los dos sistemas fuera el decimal, convendrá ejecutar en éste todas las operaciones por la costumbre que ya tenemos de hacerlas. Por la misma razon se toma el decimal como intermediario, generalmente, para pasar de un sistema á otro.

Ejemplos. 1.° Escribir el número *quinario* 431_5 en el sistema *decimal.*

Primer procedimiento.—La base antigua 5, en el nuevo sistema, decimal, vale 5; sus potencias sucesivas son las siguientes:

$$b^0 = 1, \quad b^1 = 5, \quad b^2 = 25$$

y sus productos por las cifras 1, 3, 4, en el sistema decimal, estos otros:

$$1, \quad 5 . 3, \quad 25 . 4:$$

cuya suma constituye el número que se busca, á saber:

$$431_5 = 4 . 25 + 3 . 5 + 1 = 116_{10}.$$

Segundo procedimiento.—La base nueva 10 en el sistema antiguo vale 20; ejecutando en este sistema (de base 5) las operaciones, tendremos:

4 3 1	2 0	
3 1	2 1	2 0
1 1	1	1
(6		

Y, por consecuencia, como antes: $4\,3\,1_{5} = 1\,1\,6_{10}$.

Nótese que, no alterándose la totalidad de unidades que un número contiene, porque varie su modo de ser escrito, segun el sistema de numeracion que se adopte, no habrá inconveniente en establecer la igualdad:

$$N_{10} = N_{2} = a_0 2^0 + a_1 2^1 + a_2 2^2 + \ldots$$

relativa á los sistemas decimal y binario. Y, como las cifras en este último sistema sólo pueden ser 0 y 1, es claro que la forma polinómica del número N es en realidad la suma de la progresion geométrica, completa ó incompleta,

$$2^0,\quad 2^1,\quad 2^2,\quad 2^3, \ldots\ldots :$$

de lo cual se colige que todo número decimal es una suma de potencias, sucesivas, ó no, del número 2. Así sucede, por ejemplo:

$$63_{10} = 1\,1\,1\,1\,1\,1_{2} = 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0$$

$$75_{10} = 1\,0\,0\,1\,0\,1\,1_{2} = 2^6 + 2^3 + 2^1 + 2^0$$

$$26_{10} = 1\,1\,0\,1\,0_{2} = 2^4 + 2^3 + 2^1$$

En los principios demostrados se funda el teorema que sigue:

Teorema. Si p representa un entero cualquiera, positivo, y el número N, de n cifras, se escribe en el sistema de base p, esto es:

$$N = a_0 + a_1 p + a_2 p^2 + \ldots\ldots + a_{n-1} p^{n-1}$$

el número de veces que entra el factor p en la série natural

$$1, 2, 3 \ldots\ldots N$$

está expresado por el cociente

$$\frac{N - (a_0 + a_1 + a_2 + \ldots\ldots + a_{n-1})}{p-1}$$

En efecto, dividamos la forma polinómica del número N, sucesivamente, por las potencias p^1, p^2, p^3, $\ldots\ldots p^{n-1}$; designando por $c_1, c_2, c_3, \ldots\ldots c_{n-1}$ los cocientes resultantes, se obtiene el siguiente cuadro:

$$\frac{N}{p} = c_1 + \frac{a_0}{p}$$

$$\frac{N}{p^2} = c_2 + \frac{a_0 + a_1 p}{p^2}$$

$$\frac{N}{p^3} = c_3 + \frac{a_0 + a_1 p + a_2 p^2}{p^3}$$

. . . . . .

. . . . . .

$$\frac{N}{p^{n-1}} = c_{n-1} + \frac{a_0 + a_1 p + a_2 p^2 + a_0 p^3 + \ldots\ldots + a_{n-2} p^{n-2}}{p^{n-1}}$$

La suma

$$c_1 + c_2 + c_3 + \ldots\ldots + c_{n-1} = \Sigma\,(c)$$

expresa evidentemente cuántos números existen en la série natural, $1, 2, 3, \ldots\ldots N$, divisibles por p, por p^2, por p^3, ... por p^{n-1}: ó bien, el número de factores p contenidos en ella; y la cuestion ahora queda reducida á encontrar el valor explícito de tal suma. Para esto sumemos las igualdades (1); y, teniendo presente que

$$\frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \ldots\ldots + \frac{1}{p^{n-1}} = \frac{p^{n-1} - 1}{p^{n-1}\,(p-1)},$$

y que

$$a_0 + a_1 + a_2 + \ldots\ldots + a_{n-1} = \Sigma\,(a)$$

se halla la siguiente:

$$\frac{N\,(p^{n-1}-1)}{p^{n-1}\,(p-1)} = \Sigma(c) + a_0\,\frac{p^{n-1}-1}{p^{n-1}\,(p-1)} + a_1\,\frac{p^{n-2}-1}{p^{n-2}\,(p-1)} +$$

$$+ a_2\,\frac{(p^{n-3}-1)}{p^{n-3}\,(p-1)} + \ldots\ldots$$

de la cual, separando como factor comun $\dfrac{1}{p^{n-1}\,(p-1)}$, se deduce:

$$\Sigma\,(c) = \frac{1}{p^{n-1}\,(p-1)}\left\{ p^{n-1}\,(N - \Sigma\,(a)) - N + (a_0 + a_1\,p + a_2\,p^2 + \ldots\ldots) \right\}$$

ó por fin esta otra:

$$\Sigma(c) = \frac{N - \Sigma(a)}{p-1} = \frac{N - (a_0 + a_1 + \ldots\ldots a_{n-1})}{p-1}$$

que demuestra el teorema.

Como el primer miembro de esta última igualdad es por su significado siempre entero, se desprende de la misma que la diferencia $N - \Sigma(a)$ es siempre divisible por $(p-1)$.

Ejemplos. 1.° El número decimal 73 escrito en el sistema *quinario* es 243_5; en la série natural

$$1,\ 2,\ 3 \ldots\ldots 73,$$

por consecuencia, se hallará contenido, como factor, el número 5,

$$\Sigma(c) = \frac{73 - (2+4+3)}{5-1} = 16 \text{ veces.}$$

2.° El número decimal 53_{10} es equivalente al 1222_3 en el sistema ternario: luego en la série

$$1,\ 2,\ 3,\ \ldots\ldots 53$$

se hallará contenido el factor 3

$$\Sigma(c) = \frac{53 - (1+2+2+2)}{3-1} = 23 \text{ veces.}$$

Corolario.—Si p representa un número primo, y el número N, de n cifras, se escribe en el sistema de base p, el número de veces que el factor p se halla contenido en el producto

$$N! = 1 \,.\, 2 \,.\, 3 \ldots\ldots (N-1)\, N,$$

tiene tambien por expresion el cociente

$$\frac{N-(a_0+a_1+a_2+\ldots\ldots+a_{n-1})}{p-1}.$$

En efecto: este mismo cociente expresa el número de veces que entra, como factor, el número p (aunque no sea primo) en la série 1, 2, 3, ... N.; mas no puede asegurarse que las mismas veces entrará tambien p en el producto $N!$, sin fijar de antemano que p es primo; puesto que, si p no fuese primo, sino compuesto de los factores a, b, por ejemplo, siempre existirian dos factores en $N!$: uno $\equiv a \pmod{p}$, y otro $\equiv b \pmod{p}$, cuyo producto seria $\equiv ab = p$; y, por consecuencia, el número de factores p, contenidos en aquél, sería mayor que el expresado por el cociente del teorema. No sucederá así cuando p sea primo; pues entre los restos (mod. p) de los términos de la série 1, 2, 3, ... N, no habrá entónces dos, cuyo producto sea p. Y en este caso, en el de ser p número primo, se verificará, por consecuencia, el corolario enunciado.

Ejemplo. El número decimal 42_{10} es equivalente al quinario 132_5: luego el número 5 se hallará contenido en el producto 42!

$$\frac{42-(1+3+2)}{5-1}=9 \text{ veces.}$$

2.—*Divisibilidad de los números.*

Dividamos ahora el número

$$N=a_{n-1}\ldots\ldots a_2\,a_1\,a_0=a_0+a_1\,b+a_2\,b^2+\ldots\ldots+a_{n-1}\,b^{n-1} \qquad (1)$$

escrito en el sistema de base b, por otro cualquiera, d. Designando

por $r_1, r_2 \ldots\ldots r_{n-1}$ los restos respectivos (mod. d) de las potencias sucesivas $b^1\ b^2 \ldots\ldots b^{n-1}$, de la base b, es indudable que se verificará la congruencia:

$$N \equiv (a_0 + a_1 r_1 + a_2 r_2 + \ldots\ldots + a_{n-1} r_{n-1}) \text{ (mod. } d) \qquad (2)$$

de la cual se colige, haciendo para mayor brevedad,

$$R = a_0 + a_1 r_1 + a_2 r_2 + \ldots\ldots + a_{n-1} r_{n-1}$$

que N será, ó no, divisible por d, segun que R lo sea, ó deje de serlo. Las condiciones de divisibilidad del número N por el número d se fundan, por consecuencia, en las propiedades de los restos (mod. d) de las potencias sucesivas de la base del sistema de numeracion en que estén escritos aquellos números; y, como todo lo que á dichos restos potenciales se refiere queda ya dicho en el texto (84, 85, 88), nada nuevo en realidad vamos á decir ahora; sino puramente á aplicar á la doctrina particular de la Divisibilidad los principios allí consignados.

1.° Consideremos primeramente los divisores representados, por potencias de la base, por factores de la misma, ó por potencias de estos factores.

a) Si $d = b^s$, se verificará la congruencia

$$N \equiv a_{s-1} \ldots\ldots a_2\ a_1\ a_0 \text{ (mod. } b^s);$$

y, como las cifras a son todas menores que b, y en consecuencia, $a_{s-1} \ldots\ldots a_2\ a_1\ a_0 < b^s$, resulta que, si N ha de ser divisible por b^s, las s primeras cifras de la derecha deben ser ceros.

b) Si el divisor d es un factor cualquiera, f, de la base b, será cierta la congruencia

$$N \equiv a_0 \text{ (mod. } f);$$

la cual exije que a_0 sea cero, ó múltiplo de f, para que N sea lo último.

c) Si el divisor es una potencia, f^s, de un factor f de la base, primo con los demás factores, dicho divisor, f^s, lo será de b^s, y se verificará, por lo tanto, en este caso tambien, la congruencia

$$N \equiv a_{s-1} \ldots\ldots a_2\, a_1\, a_0 \text{ (mod. } f^s\text{)},$$

la cual pide, para que N sea divisible por f^s, que las s primeras cifras de la derecha del dividendo sean ceros, ó compongan un múltiplo de f^s.

Conviene advertir que, sólo en el caso de ser el factor f, primo con todos los demás factores de la base b, se puede asegurar que su potencia, f^s, será divisor de la misma potencia, b^s, de la base, sin serlo de potencias inferiores; y tal caso ocurrirá siempre que la base contenga solamente dos factores primos, desiguales, y elevados á la primera potencia.

2.° Consideremos ahora los divisores primos con la base y, por lo tanto, con sus potencias sucesivas. Si designamos por b^ε la mínima de estas potencias congruente con la unidad (mod. d), y escribimos el número N en el sistema cuya base sea b^ε, lo cual equivale á descomponerlo en grupos de ε cifras cada uno (comenzando por la derecha naturalmente), es indudable que la congruencia (2) se convertirá en esta otra:

$$N \equiv g_\varepsilon \text{ (mod. } d\text{)}, \qquad (3)$$

representando g_ε la suma de los grupos mencionados: cada uno de los cuales significa, respecto del número N, escrito en el sistema de base b^ε, lo mismo que cada una de las cifras a de aquel número N, escrito en el sistema de base b.

Mas, si el exponente ε, á que pertenece b segun el divisor d, fuese par, no sólo se verificará, como antes, la congruencia

$$b^\varepsilon \equiv 1 \text{ (mod. } d\text{)}; \text{ sino tambien: } b^{\frac{1}{2}\varepsilon} \equiv -1 \text{ (mod. } d\text{)};$$

y entónces, descomponiendo el número N en grupos de $\frac{1}{2}\varepsilon$ cifras cada uno, y designando por $g_{\frac{1}{2}\varepsilon}$ la suma de los grupos de lugar par, y por $y_{\frac{1}{2}\varepsilon}$ la suma de los grupos de lugar impar, será cierta tambien la siguiente:

$$N \equiv (g_{\frac{1}{2}\varepsilon} - y_{\frac{1}{2}\varepsilon}) \text{ (mod. } d). \qquad (4)$$

a) Sea el divisor $d = (b-1)$, esto es, la base ménos la unidad: de la congruencia evidente

$$b \equiv 1 \text{ (mod. } (b-1))$$

se deduce $\varepsilon = 1$, y, por consecuencia:

$$N \equiv g = a_0 + a_1 + \ldots\ldots a_{n-1} \text{ (mod. } b-1).$$

La misma condicion para todo factor de $(b-1)$.

b) Sea el divisor $d = b^s - 1$; y de la congruencia entónces cierta

$$b^s \equiv 1 \text{ (mod. } (b^s - 1)),$$

se desprende esta otra:

$$N \equiv g^s \text{ (mod. } (b^s - 1))$$

aplicable tambien á cualquier factor de $(b^s - 1)$.

c) Sea el divisor $d = (b+1)$, esto es, la base más la unidad: de las congruencias consiguientes:

$$b \equiv -1 \text{ (mod. } (b+1))$$

$$b^2 \equiv +1 \text{ (mod. } (b+1))$$

se deriva la que á continuacion se expresa:

$$N \equiv (g - y) \text{ (mod. } (b+1)).$$

El mismo carácter para todo factor de $(b+1)$.

d) Sea $d=(b^s+1)$: de las congruencias

$$b^s \equiv -1 \pmod{(b^s+1)}$$

$$b^{2s} \equiv +1 \pmod{(b^s+1)}$$

se deduce la que sigue:

$$N \equiv (g_s - y_s) \pmod{(b^s+1)},$$

que expresa, como las correspondientes, anteriores, la condicion de divisibilidad del número N por (b^s+1), y, en consecuencia, por cualquier factor de (b^s+1).

A cuenta del lector corre la traduccion de las congruencias que preceden al lenguaje vulgar, así como el aplicarlas al sistema de numeracion que mejor le convenga. Sólo advertiremos que las comprendidas en el §. 1.°, tomando por base 10, indican los caracteres de divisibilidad por 10^s; por 2 y por 5; por 2^s y por 5^s; así como las del §. 2.° contienen las condiciones de divisibilidad por 9 y por 3; por $99=10^2-1$ y sus factores 3, 9, 11, 33, 99, etc.; por $11=10+1$; por $101=10^2+1$; por $1001=10^3+1$ y sus factores que son 7, 11, 13, 77, 91, 143; etc.

Para concluir diremos que la condicion de divisibilidad de un número N (de base b) por otro cualquiera, d, puede hallarse, en general, descomponiendo este divisor d en sus factores primos; y la condicion que se busca será la reunion de las concernientes á estos factores primos.

ÍNDICE.

PARTE PRIMERA.

Principios fundamentales de la teoría de los números.

CAPÍTULO I.

DE LA ARITMÉTICA PROPIAMENTE DICHA.—CÓMO SE CONSIDERAN Y ESTUDIAN LOS NÚMEROS EN ESTA PARTE DE LA MATEMÁTICA.

	Págs.
1—*Magnitud, cantidad, número*	1
2—*Números enteros, fraccionarios é inconmensurables*	2
3—Aritmética.—*Su objeto*	3
4—Operaciones de cálculo.—*Séries fundamentales*	3
5—*Adicion*	4
6—*Multiplicacion*	4
7—*Sustraccion*	5
8—*Números negativos*	5
9—*Division*	7
10—*Números fraccionarios*	7
11—*Elevacion á potencias*	8
12—*Extraccion de raices*	10
13—*Números irracionales*	10
14—*Cálculo logarítmico*	11

Pags.

15—*Gradacion de las operaciones de cálculo*..... 12
16—*Conceptos diferentes del número*..... 17
17—*Leyes formales.—Principio de su permanencia*..... 20
18—*Aplicacion de las leyes formales*..... 22
19—Operaciones coordinatorias. *Definiciones.—Notacion*..... 28
20—*Número de variaciones sin repeticion*..... 29
21—*Número de permutaciones sin repeticion*..... 30
22—*Número de combinaciones sin repeticion*..... 31
23—*Número de combinaciones con repeticion*..... 33
24—*Número de variaciones con repeticion*..... 34
25—*Número de permutaciones con repeticion*..... 35
26 —*Relaciones entre números coordinatorios*..... 37
27—*Número de todas las combinaciones posibles*..... 38
28—Potencia de un binomio.—*Preliminares*..... 40
29—*Desarrollo simbólico de un binomio*..... 44
30—*Séries binomias.—Definicion*..... 46
31—*Producto de séries binomias*..... 47
32—*Potencia de una série binomia*..... 48
33—*Potencia de un binomio*..... 48
34—*Potencia de un polinomio*..... 50

CAPÍTULO II.

DE LA TEORÍA DE LOS NÚMEROS.—CÓMO SE CONSIDERAN Y ESTUDIAN LOS NÚMEROS EN ESTA PARTE DE LA MATEMÁTICA.

35—*Ideas generales*..... 52
36—*Números figurados*..... 55
37—*Números poligonales*..... 56
38—*Clasificacion de los números.—Objeto concreto de su Teoría*.. 57

CAPÍTULO III.

DE LA DIVISIBILIDAD DE LOS NÚMEROS.

Págs.

39—*Proposiciones elementales* 61
40—*Máximo comun divisor de dos números* 63
41—*Números primos entre sí.—Teorema fundamental* 65
42—*Máximo comun divisor de varios números* 67
43—*Mínimo comun múltiplo de dos números* 70
44—*Mínimo comun múltiplo de varios números* 72
45—*Números primos absolutos* 74
46—*Números compuestos.—Teorema fundamental* 75
47—*Forma de los divisores de un número* 77
48—*Multitud de todos los divisores de un número* 78
49—*Suma de todos los divisores de un número* 79
50—*Determinacion del máximo comun divisor y mínimo comun múltiplo de varios números mediante sus factores primos* 80
51—*Ley de Euler* 82
52—*Números amigables* 91
53—*Números perfectos* 94
54—*Máxima potencia de un número primo contenida en el producto* $n! = 1 . 2 . 3 \ldots . n$ 97
55—*De los números primos con otro dado é inferiores á éste. Funcion* $\varphi(N)$ 101
56—*Demostracion de la ley* $\varphi(NN') = \varphi(N)\,\varphi(N')$, *cuando* N *y* N' *son primos entre sí* 105
57—*Demostracion de la ley* $\sum \varphi(D) = N$, *en la cual* D *representa todos los divisores del número* N 107
58—*Nueva deduccion de la funcion* φ *de un modo más general* ... 110

CAPÍTULO IV.

DE LA CONGRUENCIA DE LOS NÚMEROS.

Págs.

59—*Definiciones* 117
60—*Restos y no-restos de un módulo* 119
61—*Propiedades de los números congruentes* 121
62—*Sistemas completos de números incongruentes* 127
63—*Proposiciones fundamentales* 129
64—*Teorema de Euler* 132
65—*Teorema de Fermat* 136
66—*Otra demostracion de estos mismos teoremas* 137

PARTE SEGUNDA.

Resolucion de las congruencias.

CAPITULO I.

DE LAS CONGRUENCIAS DE PRIMER GRADO.

67—*Definiciones generales* 141
68—*Congruencias de primer grado. Resolucion: primer método* 144
69—*Segundo método* 149
70—*Demostracion de la fórmula* $ax+by+cz+\ldots\ldots=\delta$, *donde* δ *representa el máximo comun divisor de los números* a, b, c, ... 154

Págs.

71—*Hallar los números congruentes con dos números dados, respecto de dos módulos dados*..... 155
72—*Hallar los números congruentes con varios números dados, respecto de varios módulos dados*..... 157
73—*Descomposicion de una fraccion en la suma de otras más sencillas.* 164
74—*Resolucion de varias congruencias de primer grado con igual número de incógnitas*.. 167

CAPÍTULO II.

PROPOSICIONES GENERALES SOBRE LAS CONGRUENCIAS.

75—*Congruencia con cero del producto de dos funciones*..... 174
76—*Descomposicion de una funcion entera en otras dos*..... 175
77—*Composicion del primer miembro de una congruencia*..... 177
78—*Número máximo de raices de una congruencia* 179
79—*Relaciones entre las raices de dos congruencias y las correspondientes á su producto*..... 180
80—*Criterio de las soluciones enteras*..... 181
81—*Teorema de Wilson para los números primos, absolutos*..... 183

CAPÍTULO III.

DE LAS CONGRUENCIAS BINOMIAS.

82—*Preliminares*..... 184
83—De las raices primitivas. *Su existencia*..... 187
84—*De los números pertenecientes á un exponente dado, respecto de un módulo primo, impar*..... 190
85—*De las raices primitivas de un módulo primo, impar*..... 193
86—*Método para hallar las raices primitivas de un número primo, impar*..... 197

Págs.

87—*Otro método para obtenerlas*..... 198
88—*Complemento de la doctrina general anterior*..... 203
89—*De los índices para estos módulos*..... 209
90—*Propiedades de los índices*..... 210
91—*Uso de las tablas de índices, ó* Canon arithmeticus, *para resolver las congruencias de primer grado*..... 214
92—*De las raices primitivas de una potencia, superior á la primera, de un número primo impar, ó del duplo de tal potencia*..... 216
93—*De los índices para estos módulos*..... 223
94—*De las raices primitivas de una potencia cualquiera del número primo* 2.—Índices..... 225
95—*De las raices primitivas de un número compuesto cualquiera* .. 229
96—Resolucion de la congruencia binomia de módulo primo. *Enunciado del problema*..... 230
97—*Resolucion por el* Canon arithmeticus..... 231
98—*Resolucion directa. Posibilidad y número de sus soluciones*.... 233
99—*Número de sus restos potenciales*..... 236
100—*Modo de hallar sus soluciones ó raices*..... 238
101—Resolucion de la congruencia binomia de módulo cualquiera. 244
102—*Observacion* 249

CAPÍTULO IV.

DE LAS CONGRUENCIAS DE SEGUNDO GRADO.

103—*Restos cuadráticos. Las dos partes de su teoría*..... 251
104—Primera parte.—*Carácter de un número primo impar, deducido directamente.—Símbolo de* Legendre..... 252
105—*Trasformacion del carácter precedente*..... 256
106—Estudio general del asunto.—*De la congruencia* $x^2 \equiv D \pmod{k}$ *cuando* k *sea un número primo impar*..... 262
107—*De la congruencia* $x^2 \equiv D \pmod{k}$, *cuando* k *sea una potencia cualquiera de un número primo impar*..... 263

Págs.

108—*De la congruencia* $x^2 \equiv D \pmod{k}$, *cuando* k *sea una potencia, superior á la primera, del número* 2 267
109—*De la congruencia* $x^2 \equiv D \pmod{k}$, *cuando* k *sea un número cualquiera* 271
110—*Teorema generalizado de Wilson* 273
111—Segunda parte.—*Verdadero concepto del asunto. Símbolos que comprende* 275
112—*Determinacion del símbolo* $\left(\frac{-1}{p}\right)$ 277
113—*Determinacion del símbolo* $\left(\frac{2}{p}\right)$ 280
114—*Demostracion más general de este caracter* 285
115—*Determinacion del símbolo* $\left(\frac{q}{p}\right)$. *Ley de reciprocidad* 287
116—*Aplicacion de esta ley á casos particulares* 294
117—*Aplicacion de la misma para determinar en general el símbolo de Legendre* 297
118—*Generalizacion de este símbolo por Jacobi* 301
119—*Relacion entre los símbolos de Legendre y de Jacobi. Ley de reciprocidad generalizada* 304
120—*Aplicacion de esta ley para determinar el símbolo de Jacobi* .. 309
121—Formas lineales de los divisores de $t^2 - Du^2$. *Sus cuatro casos* 313

CAPÍTULO V.

DE LA DIVISION DEL CÍRCULO.

122—*Planteamiento del problema* 324
123—Ecuacion de la division del círculo. *Preliminares indispensables para su resolucion* 332
124—1.°—*Relacion entre dos ecuaciones, siendo las raices de una de ellas las potencias* p^{r} *de las raices de la otra* 335

Págs.

125—2.°—*La ecuacion de la division del círculo irreducible*..... 340
126—Método de Gauss para resolver la ecuacion del círculo.—*Sus fundamentos. Orden entre las raices de dicha ecuacion*..... 350
127—*Reduccion de las funciones de estas raices á la forma* normal. 352
128—*Distribucion de las mismas raices en períodos* f-membres, *siendo el grado de la ecuacion,* p—1=ef..... 354
129—*Forma lineal de sus funciones enteras*..... 359
130—*De la ecuacion irreducible, cuyas raices son los períodos* f-membres..... 364
131—*De la ecuacion irreducible, cuyas raices son los términos de un período* f-membre. *Descomposicion nueva de estos períodos en otros* f'-membres, *siendo* p—1=ee'f'..... 367
132—*De la ecuacion irreducible, cuyas raices son los* e' *períodos que componen uno* f-membre. *Regla final*..... 370
133—*Casos en que puede dividirse la circunferencia con la regla y el compás.—Distribucion conveniente de* (p—1) *en sus factores*..... 373
133—Ejemplos.—1.° *Dividir la circunferencia en* 5 *partes iguales. Construccion.*—2.° *Dividir la circunferencia en* 13 *partes iguales.*—3.° *Dividir la circunferencia en* 17 *partes iguales. Construccion*..... 375

PARTE TERCERA.

Teoría de las formas cuadráticas.

CAPITULO I.

DE LA TRASFORMACION Y EQUIVALENCIA DE LAS FORMAS CUADRÁTICAS EN GENERAL.

134—*Preliminares y definiciones*..... 391
135—*Trasformacion ó sustitucion simple: propia é impropia*..... 393
136—*Trasformacion ó sustitucion compuesta: propia é impropia*... 396

Págs.

137—*Equivalencia de las formas: propia é impropia.—Formas* opuestas, socias, *y* contíguas.—*Formas* ambíguas (ancípites). *Siempre existe una forma ambígua, equivalente á cualquiera otra forma que sea del modo impropio equivalente á sí misma*..... 399

CAPÍTULO II.

DE LA EQUIVALENCIA DE LAS FORMAS EN PARTICULAR.—SUS DOS PROBLEMAS FUNDAMENTALES.

138—*Clasificacion de las formas.—Sistema completo de formas no-equivalentes*..... 409
139—*Enunciado de los dos problemas fundamentales de las equivalencias.—Construcciones propias é impropias de los números. Su relacion íntima con dichos problemas*..... 410

CAPÍTULO III.

DEL SEGUNDO PROBLEMA DE LAS EQUIVALENCIAS PARA LAS DETERMINANTES NEGATIVAS.

140—*Razon de anticiparlo al primero.—Primera reduccion del mismo. Divisores de las formas y de las clases. Formas* primitivas, *de* primera *y* segunda especie, *y* derivadas..... 416
141—*Segunda reduccion.*—Ecuacion de Pell..... 420
142—*Resolucion de esta ecuacion para las determinantes negativas, y terminacion consiguiente para estas determinantes del segundo problema de las equivalencias*..... 424

CAPÍTULO IV.

DEL PRIMER PROBLEMA DE LAS EQUIVALENCIAS PARA LAS DETERMINANTES NEGATIVAS.

143—*Limitaciones que exije este problema en las formas.—Formas* reducidas..... 427

Págs.

144—*Equivalencia entre una forma cualquiera, con determinante negativa, y otra forma reducida*..... 429
145—*Equivalencia entre dos formas reducidas*..... 432
146—*Resúmen aclaratorio*..... 436
147—*El número de clases de formas no-equivalentes, para una determinante negativa, es finito*..... 437
148—*Aplicaciones de la doctrina precedente á la representacion de los números por formas determinadas. Ejemplos*..... 442

CAPÍTULO V.

DEL PRIMER PROBLEMA DE LAS EQUIVALENCIAS PARA LAS DETERMINANTES POSITIVAS.

149—*Preliminares.—Raices, primera y segunda, de una forma*... 456
150—*Dependencia entre dos raices de dos formas equivalentes.—Aplicacion á las formas contiguas*..... 458
151—*Nuevas formas reducidas: propiedades de sus raices*..... 461
152 *El número de formas reducidas, correspondientes á una determinante positiva, dada, es finito*..... 464
153—*Equivalencia entre una forma cualquiera, con determinante positiva, y otra forma reducida.—El número de clases de formas no-equivalentes, para una determinante positiva, es tambien finito.* 467
154—*Equivalencia entre dos formas reducidas.—Siempre existe una sola forma, contigua de una reducida, que es tambien reducida*.... 471
155—*Distribucion en períodos de las formas reducidas, correspondientes á una determinante positiva*..... 473
155 *—Períodos de las formas socias y ancípites*..... 478
156—*Desarrollo en fraccion continua de las raices de las formas reducidas, con determinante positiva*..... 480
157—*Conclusion del primer problema de las equivalencias para las determinantes positivas*..... 485

CAPÍTULO VI.

DEL SEGUNDO PROBLEMA DE LAS EQUIVALENCIAS PARA LAS DETERMINANTES POSITIVAS.

Págs.

158—*Resolucion de la* ecuacion de Pell *para las determinantes positivas* 489
159—*Solucion mínima de esta ecuacion.—Fórmula general* 498
160—*Reduccion á la forma* pelliana *de la ecuacion general, binaria, de segundo grado* 506

CAPÍTULO VII.

DEL NÚMERO DE CLASES EN QUE PUEDEN DISTRIBUIRSE LAS FORMAS CUADRÁTICAS, BINARIAS, CON UNA DETERMINANTE CONOCIDA.

161—*Caracteres de los números susceptibles de ser representados por un sistema completo de formas primitivas.—Grupos de construcciones* 510
162—*Número de estas construcciones.—Recapitulacion* 512
163—*Ecuacion fundamental.—Sumas principales* 518
164—*Trasformacion de su segundo miembro* 519
165—*Modificacion de dicha ecuacion para que pueda ser tambien satisfecha por construcciones impropias* 524
166—*Consecuencias interesantes de la doctrina precedente* 527
167—*Restricciones que deben imponerse á las formas representantes de las clases* 536
168—*Distribucion de los números constructores en un número determinado de séries aritméticas, pareadas* 539
169—*Límite del primer miembro de la ecuacion fundamental para las determinantes negativas* 545

Págs.

170—*Límite del segundo miembro. Número de clases de formas para las determinantes negativas, expresado simbólicamente*..... 549
171—*Relacion entre los números de clases de formas primitivas, de la primera, y de la segunda especie, para una determinante negativa.* 551
172—*Límite del primer miembro de la ecuacion fundamental para las determinantes positivas.—Expresion simbólica del número de clases de formas para estas determinantes* 553
173—*Relacion entre los números de clases de formas primitivas, de la primera y de la segunda especie, para una determinante positiva.* 559
174—*Reduccion del problema, objeto de este capítulo, al caso de una determinante, no divisible por ningun cuadrado, sea aquélla negativa ó positiva*..... 562
175—*Convergencia y continuidad de la série abreviada que figura en la expresion simbólica del número de clases de formas para unas y otras determinantes*..... 567
176—*Suma de esta série de los cuatro casos que pueden ocurrir.—Suma en el primer caso*..... 573
177—*Suma en todos los casos*..... 585
178—*Fórmulas finales para determinar el número de clases que buscamos*..... 597

APÉNDICES.

I. —DE LAS FRACCIONES CONTÍNUAS.

1—ALGORITMO DE EULER. *Sus leyes principales.—Aplicacion*..... 607
2—FRACCIONES CONTÍNUAS.—a) *Definiciones; notacion; concordancia de este nuevo símbolo con el del algoritmo de Euler.*—b) *Fracciones aproximadas.*—c) *Propiedades de las aproximadas; por qué se llaman* reducidas.—d) *Fracciones contínuas infinitas; su convergencia.*—e) *Conversion de una fraccion contínua,* irregular, *en otra* regular.—f) *Demostracion de un teorema importante, relativo á las mismas*..... 614

II.—LÍMITE DE UNA SÉRIE INFINITA.

Págs.

1—*Caso particular* 629
2—*Caso general*..... 631

III.—ESTUDIO DE UNA LEY GEOMÉTRICA.

1—*Límite de un producto*..... 636

IV.—ALGUNAS PROPOSICIONES DE GAUSS REFERENTES Á SU TEORÍA DE LA DIVISION DEL CÍRCULO.

1—*Lema concerniente á las séries de Fourier*..... 640
2—*Valor de la suma* $\varphi(h, n)$ *para* $n \equiv 0 \pmod 4$ *y* $h = 1$... 643
3—*Leyes generales de las sumas* $\varphi(h, n)$.... 649
4—*Determinacion general de la suma* $\varphi(1, n)$..... 652
5—*Determinacion general de* $\varphi(h, n)$..... 654
6—*Demostracion de una fórmula empleada en el texto*..... 658

V.—SOBRE LOS SISTEMAS DE NUMERACION, Y LA DIVISIBILIDAD DE LOS NÚMEROS.

1—*Expresion de un número en sistemas diferentes de numeracion*.. 664
2—*Divisibilidad de los números*..... 670

3 2044 093 250 595